

Kūrėjų programos politika

(įsigaliojimo data: 2024 m. rugpjūčio 31 d., jei nenurodyta kitaip)

Sukurkime patikimiausią pasaulyje programų ir žaidimų šaltinį

Jūsų kuriamos naujovės padeda mums visiems kartu klestėti, bet su sėkme ateina atsakomybė. Ši Kūrėjų programos politika kartu su [Kūrėjų platinimo sutartimi](#) užtikrina, kad kartu mes ir toliau daugiau nei milijardui žmonių sistemoje „Google Play“ teiksime pačias moderniausias ir patikimiausias programas. Raginame jus ir toliau skaityti mūsų pateiktą politiką.

Apribotas turinys

Žmonės visame pasaulyje kasdien naudoja „Google Play“, kad pasiektų programas ir žaidimus. Prieš pateikdami programą apsvarstykite, ar ji tinkama sistemai „Google Play“ ir atitinka vietinius įstatymus.

Pavojus vaikams

Programos, kuriose naudotojams nėra draudžiama kurti, įkelti ar platinti su vaikų išnaudojimu ar prievarta prieš vaikus susijusio turinio, bus iš karto pašalintos iš „Google Play“. Tai apima visą seksualinės prievartos prieš vaikus medžiagą. Norėdami pranešti apie „Google“ produkto turinį, kuriame gali būti išnaudojamas vaikas, spustelėkite [Pranešti apie piktnaudžiavimą](#). Jei kur nors internete pastebite tokį turinį, kreipkitės tiesiogiai į [atitinkamą instituciją savo šalyje](#).

Draudžiame naudoti programas, siekiant kelti pavojų vaikams. Tai apima programų naudojimą siekiant skatinti prieš vaikus nukreiptą grobuonišką elgseną, kaip nurodyta toliau (bet tuo neapsiribojama).

- Netinkamas elgesys su vaiku (pvz., grabinėjimas ar glamonėjimas).
- Vaikų viliojimas (pvz., susidraugavimas su vaiku internetu, siekiant internetu arba ne internetu užmegzti seksualinio pobūdžio kontaktą ir (arba) keistis seksualinio pobūdžio vaizdais su tuo vaiku).
- Nepilnamečių seksualizavimas (pvz., vaizdų, kuriuose vaizduojama, skatinama ar reklamuojama seksualinė prievarta prieš vaikus arba vaikai vaizduojami taip, kad gali būti imtasi seksualinio vaikų išnaudojimo).
- Seksualinis prievartavimas (pvz., grasinimas vaikui ar jo šantažavimas naudojant realią arba tariamą prieigą prie vaiko intymių vaizdų).
- Prekyba vaikais (pvz., vaiko reklamavimas arba siūlymas seksualiai išnaudoti komerciniais tikslais).

Aptikę turinio, kuriame yra seksualinės prievartos prieš vaikus medžiagos, imsimės atitinkamų veiksmų, kurie gali apimti pranešimą Nacionaliniam dingusių ir išnaudojamų vaikų centrui. Jei manote, kad vaikui gresia prievarta, išnaudojimas ar prekyba žmonėmis arba jis tapo šių veiksmų auka, kreipkitės į vietinę teisės saugos instituciją ir [čia](#) nurodytą vaikų saugos užtikrinimo organizaciją.

Be to, neleidžiamos programos, skirtos vaikams, bet kuriose yra suaugusiems skirtų temų, įskaitant nurodytas toliau (bet jomis neapsiribojant).

- Programos, kuriose yra daug smurto, kraujo ir kruvinų smurto scenų.
- Programos, kuriose vaizduojama arba skatinama žalinga ir pavojinga veikla.

Taip pat neleidžiame teikti programų, kuriose reklamuojamas neigiamas kūno ar savęs vaizdas, įskaitant programas, kuriose pramoginiais tikslais vaizduojama plastinė chirurgija, svorio metimas ir kiti kosmetiniai asmens fizinės išvaizdos koregavimai.

Netinkamas turinys

Siekdami užtikrinti, kad „Google Play“ būtų saugi ir tinkama platforma, sukūrėme standartus, apibrėžiančius ir draudžiančius naudotojams žalingą ar netinkamą turinį.

Seksualinis turinys ir nešvankybės

Neleidžiame programų, kuriose teikiamas ar reklamuojamas seksualinis turinys ar nešvankybės, įskaitant pornografiją, arba turinys ar paslaugos, skirti seksualiniam malonumui teikti. Neleidžiame programų ar jų turinio, kurie atrodo kaip reklamuojantys ar siūlantys seksualinių paslaugų teikimą už atlygį. Neleidžiame programų, kuriose teikiamas ar reklamuojamas turinys, susijęs su seksualiai grobuoniška elgsena, ar platinamas santykių, nesant abiejų partnerių sutikimo, seksualinis turinys. Turinys, kuriame yra nuogybių, gali būti teikiamas, jei jo pagrindinis tikslas yra mokomojo, dokumentinio, mokslinio ar meninio pobūdžio ir jei toks turinys teikiamas pagrįstai.

Katalogų programose (programose, kuriose knygų ir (arba) vaizdo įrašų pavadinimų sąrašai teikiami kaip platesnio turinio katalogo dalis) gali būti platinami knygų (įskaitant el. knygas ir garsines knygas) ar vaizdo įrašų pavadinimai, kuriuose yra seksualinio turinio, jei atitinkami toliau pateikti reikalavimai.

- Knygų ir (arba) vaizdo įrašų pavadinimai, kuriuose yra seksualinio turinio, sudaro nedidelę dalį viso programos katalogo.
- Programoje nėra aktyviai reklamuojami knygų ir (arba) vaizdo įrašų pavadinimai, kuriuose yra seksualinio turinio. Tokie pavadinimai vis tiek gali būti rodomi rekomendacijose, teikiamose pagal naudotojo istoriją arba per įprastus nuolaidų laikotarpius.
- Programoje neplatinami knygų ir (arba) vaizdo įrašų pavadinimai, kuriuose yra pavojų vaikui vaizduojančio turinio, pornografinio ar kitokio seksualinio turinio, pagal taikomus įstatymus apibūdinamo kaip neteisėtas.
- Programoje nepilnamečiai saugomi ribojant prieigą prie knygų ir (arba) vaizdo įrašų pavadinimų, kuriuose yra seksualinio turinio.

Jei programoje yra turinio, kuris pažeidžia šią politiką, bet konkrečiame regione laikomas tinkamu, programa gali būti pasiekama naudotojams tame regione ir būti nepasiekama naudotojams kituose regionuose.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Nuogybių ar seksualinio pobūdžio pozų vaizdai, kai subjektas yra nuogas, sulietas arba minimaliai apsirengęs ir (arba) kai apranga nepriimtina esant atitinkamam viešajam kontekstui.
- Lytinių aktų vaizdavimas, animacijos ar iliustracijos, seksualinio pobūdžio pozos ar seksualinio pobūdžio kūno dalių vaizdai.
- Turinys, kuriame vaizduojamos arba teikiamos funkcinės pagalbinės sekso priemonės, sekso vadovai, nelegalios seksualinės temos ir fetišas.
- Nepadorus ar nešvankus turinys, įskaitant (bet tuo neapsiribojant) turinį, kuriame parduotuvės įrašė arba programoje gali būti nešvankybų, užgauliojimų, nepadoraus teksto, suaugusiems skirtų ir (arba) seksualinio pobūdžio raktinių žodžių.
- Turinys, kuriame vaizduojama, aprašoma ar skatinama zoofilija.
- Programos, reklamuojančios ar siūlančios seksualinio pobūdžio pramogas, palydovų (-ių) paslaugas ar kitas paslaugas, kurios gali būti laikomos seksualinėmis paslaugomis už atlygį, įskaitant (bet tuo neapsiribojant) pasimatymus už atlygį ar lytinius aktus, kai tikimasi ar numanoma, kad vienas dalyvis sumokės, nupirks dovanų, teiks finansinę paramą kitam dalyviui (santykiai su pagyvenusiais turtingais jaunų partnerių garbintojais).
- Programos, kuriose žeminami ar įžeidžiami žmonės, pvz., programos, kurios nurodomos kaip nurengiančios žmones ar matančios per drabužius, net jei jos pažymimos kaip pokštų ar pramogų programos.
- Turinys ar elgsena, kuriais bandoma grasinti žmonėms ar juos seksualiai išnaudoti, pvz., slapta darytos nuotraukos, paslėpta kamera, santykių, nesant abiejų partnerių sutikimo, seksualinis turinys, sukurtas naudojant sintetinę vaizdakaitos ar panašią technologiją, arba seksualinės prievartos turinys.

Neapykanta

Neleidžiame teikti programų, kuriose skatinamas smurtas ar neapykanta asmenims ar grupėms dėl jų rasės ar etninės kilmės, religijos, negalios, amžiaus, tautybės, veterano statuso, seksualinės orientacijos, lyties, lytinės tapatybės, kastos, imigracijos būsenos ar kitų savybių, susijusių su sisteminė diskriminacija ar menkinimu.

Programos, kuriose yra su naciais susijusio EDSA (mokomojo, dokumentinio, mokslinio ar meninio) turinio, gali būti blokuojamos tam tikrose šalyse pagal vietinius įstatymus ir nuostatas.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Turinys ar kalba, kuriuose tvirtinama, kad saugoma grupė yra nežmogiška, žemesnio lygio arba nusipelnusi būti nekenčiama.
- Programos, kuriose pateikiama neapykantą skatinančių užgauliojimų, stereotipų ar teorijų apie saugomos grupės turimus neigiamus bruožus (pvz., piktybinė, korumpuota, žalinga ir pan.) arba aiškius ar numanomas tvirtinimus, kad grupė kelia grėsmę.
- Turinys arba kalba, kuria kiti žmonės skatinami patikėti, kad tam tikrų žmonių reikėtų nekęsti ar juos reikėtų diskriminuoti, nes jie yra saugomos grupės nariai.
- Turinys, kuriuo reklamuojama neapykantos simbolika, pvz., vėliavos, simboliai, skiriamieji ženklai, atributika, ar su neapykantos grupėmis susijusi elgsena.

Smurtas

Neleidžiame teikti programų, kuriose vaizduojamas ar skatinamas nepagrįstas smurtas ar kita pavojinga veikla. Programos, kuriose žaidžiant vaizduojamas išgalvotas smurtas, pvz., animaciniai filmai, medžioklė ar žvejyba, paprastai leidžiamos.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Tikroviški smurto ar grasinimų smurtu asmeniui ar gyvūnui vaizdai ar aprašai.
- Programos, kuriose skatinamas savęs žalojimas, savižudybė, valgymo sutrikimai, dusinimo žaidimai ar kiti veiksmai, dėl kurių galima rimtai susižeisti ar mirti.

Smurtinis ekstremizmas

Neleidžiame teroristinių organizacijų bei kitų pavojingų organizacijų ar judėjimų atstovams, susijusiems su smurto prieš civilius veiksmais, rengiantiems tokius veiksmus ar prisiimantiems už juos atsakomybę, skelbti programų sistemoje „Google Play“ bet kokiais tikslais, įskaitant verbavimą.

Neleidžiame programų, kurių turinys yra susijęs su smurtiniu ekstremizmu arba kuriame reklamuojami teroristiniai veiksmai, skatinamas smurtas ar šlovinamos teroristinės atakos. Jei su smurtiniu terorizmu susijusį turinį skelbiate turėdami švietėjiškų, mokslinių ar meninių tikslų arba siekdami kurti dokumentiką, nepamirškite pateikti atitinkamą ŠDMM kontekstą.

Delikatūs įvykiai

Neleidžiame programų, kuriose bandoma pasipelnyti iš visuomenę jaudinančio, su socialine, kultūrine ar politine veikla itin susijusio įvykio, pvz., civilinės kritinės padėties, stichinių nelaimių, visuomenės sveikatos krizių, konfliktų, mirčių ar kitų tragiškų įvykių, ar kuriose netinkamai pateikiami tokie įvykiai. Programos, kurių turinys susijęs su visuomenę jaudinančiu įvykiu, paprastai leidžiamos, jei tas turinys yra ŠDMM (švietėjiško, dokumentinio, mokslinio ar meninio) pobūdžio arba kai siekiama įspėti naudotojus apie visuomenę jaudinantį įvykį ar didinti žinomumą apie jį.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Jautrumo stoka mirus realiam žmogui ar grupei žmonių, kai nusižudoma, perdozuojama, yra natūralios priežastys ir pan.

- Tinkamai dokumentuoto, svarbaus tragiško įvykio neigimas.
- Siekiama pasipelnyti iš visuomenę jaudinančio įvykio nieko realaus nesuteikiant aukoms.

Patyčios ir priekabiavimas

Neleidžiame teikti programų, kuriose grasinama, priekabiuojama ar tyčiojama ar skatinamas toks elgesys.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Tyčiojimasis iš tarptautinių ar religinių konfliktų aukų.
- Turinys, kuriuo siekiama išnaudoti kitus, įskaitant prievartavimą, šantažą ir pan.
- Turinio skelbimas siekiant ką nors viešai pažeminti.
- Priekabiavimas prie tragiško įvykio aukų ar jų draugų ir šeimos narių.

Pavojingi produktai

Neleidžiame teikti programų, kuriomis lengviau parduoti sprogmenis, šaunamuosius ginklus, šaudmenis ar tam tikrus šaunamųjų ginklų priedus.

- Ribojami priedai apima tuos, kuriais galima šaunamaisiais ginklais simuliuoti automatinę ugnį ar paversti šaunamąjį ginklą automatinio (pvz., smūgiams skirti apsodai, automatiniai paleidikliai, automatiniai nuleistukai, keitimo rinkiniai), ir dėtuves bei diržai, kuriuose telpa daugiau nei 30 šovinių.

Neleidžiame teikti programų, kuriose pateikiamos instrukcijos, kaip pasigaminti sprogmenis, šaunamuosius ginklus, šaudmenis, ribojamus šaunamųjų ginklų priedus ar kitus ginklus. Tai apima instrukcijas, kaip paversti šaunamąjį ginklą automatinio ar simuliuotu automatinio, keičiant šaudymo galimybes.

Marihuana

Neleidžiame teikti programų, kuriomis skatinamas marihuanos ar marihuanos produktų pardavimas, neatsižvelgiant į teisėtumą.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Leidimas naudotojams užsisakyti marihuanos naudojant prekių krepšelio programoje funkciją.
- Pagalba naudotojams planuojant marihuanos pristatymą ar pasiėmimą.
- Produktų, kuriuose yra tetrahidrokanabinolio, įskaitant produktus, pvz., kanabidiolį, kuriuose yra tetrahidrokanabinolio, pardavimo palengvinimas.

Tabakas ir alkoholis

Neleidžiame teikti programų, kuriomis lengviau parduoti tabaką ar produktus su nikotinu (pvz., elektronines cigaretes, garintuvus ir nikotino maišelius) ar skatinamas neatsakingas alkoholio, tabako arba nikotino vartojimas.

Papildoma informacija

- Neleidžiama vaizduoti ar skatinti alkoholio ar tabako naudojimo ar pardavimo nepilnamečiams.
- Neleidžiama teigti, kad vartojant tabaką gali pagerėti socialinė, seksualinė, profesinė padėtis, intelektas ar fizinis pasirengimas.
- Neleidžiama skatinti nesaikingo alkoholio vartojimo, įskaitant palankų besaikio gėrimo, išgertuvių arba gėrimo varžybų vaizdavimą.
- Neleidžiama rodyti tabako produktų skelbimų, reklamų ar reikšmingų funkcijų (įskaitant skelbimus, reklamjuostes, kategorijas ir nuorodas į tabaką parduodančias svetaines).

- Galime leisti ribotą tabako produktų pardavimą maisto prekių pristatymo programose tam tikruose regionuose, taikant amžiaus tikrinimo apsaugos priemones (pvz., asmens tapatybės dokumentų patikrą pristatant).
 - Galime leisti produktų, kurie reklamuojami kaip pagalbiniai nikotino atsisakymo produktai, taikant amžiaus tikrinimo apsaugos priemones, pardavimą.
-

Finansinės paslaugos

Neleidžiame programų, kuriose naudotojams teikiami apgaulingi ar žalingi finansiniai produktai ir paslaugos.

Pagal šią politiką finansiniais produktais ir paslaugomis laikome tuos, kurie yra susiję su pinigų ir kriptovaliutų tvarkymu ar investavimu, įskaitant asmenines konsultacijas.

Jei jūsų programoje yra finansinių produktų ir paslaugų arba tokie produktai ar paslaugos reklamuojami, turite laikytis regiono ar šalies, pagal kurį (-ią) taikoma programa, nacionalinių ir vietos nuostatų. Pavyzdžiui, įtraukti paskelbimus, kurių reikalaujama pagal vietos įstatymus.

Visoms programoms, kuriose yra finansinių funkcijų, reikia užpildyti finansinių funkcijų deklaracijos formą sistemoje „[Play Console](#)“.

Binariniai opcionai

Neleidžiame programų, kuriose naudotojams suteikiama galimybė prekiauti binariniais opcionais.

Asmeninės paskolos

Asmeninės paskolos apibrėžiamos kaip fizinio asmens, organizacijos ar subjekto individualiam klientui neperiodiškai skolinami pinigai, reikalingi ne ilgalaikio turto pirkimui ar mokymuisi finansuoti.

Asmenines paskolas imantiems klientams reikia pateikti informacijos apie skolinamų produktų kokybę, savybes, mokesčius, paskolos padengimo tvarkaraštį, riziką ir pranašumus, kad jie galėtų priimti pagrįstus sprendimus, susijusius su paskolų ėmimu.

- Pavyzdžiai: asmeninės paskolos, avansu suteikiamos paskolos, jungtinio finansavimo paskolos, paskolos su užstatu.
- Neįtraukiamų paskolų pavyzdžiai: nekilnojamojo turto paskolos, paskolos automobiliams, atnaujinamosios kredito linijos (pvz., kredito kortelės, asmeninių kreditų linijos).

Programų, kuriose teikiamos asmeninės paskolos, įskaitant programas (bet jomis neapsiribojant), kurios teikia paskolas tiesiogiai, potencialių klientų generavimo programas ir programas, kurios klientams padeda susisiekti su trečiosios šalies kreditoriais, kategorija sistemoje „[Play Console](#)“ turi būti nustatyta į „Finansai“ ir jų metaduomenyse turi būti pateikta toliau nurodyta informacija.

- Minimalus ir maksimalus paskolos padengimo laikotarpiai
- Didžiausia metinė palūkanų norma (MPN), kuri paprastai apima metinę palūkanų normą ir kitus mokesčius, arba kita panaši norma, apskaičiuota laikantis vietos įstatymų
- Bendro paskolos mokesčio, apimančio pagrindinius ir visus taikomus mokesčius, pavyzdys
- Privatumo politika, kurioje išsamiai atskleidžiama informacija apie prieigą prie asmeninių ir neskelbtinų naudotojų duomenų, jų rinkimą, naudojimą ir bendrinimą, taikoma šioje politikoje apibrėžtiems apribojimams.

Neleidžiame teikti programų, kuriose reklamuojamos asmeninės paskolos, kurias reikia grąžinti per 60 arba mažiau dienų nuo paskolos išdavimo (tokias paskolas vadiname trumpalaikėmis asmeninėmis paskolomis).

Bus svarstomos politikos išimtys, susijusios su asmeninių paskolų programomis, veikiančiomis šalyse, kuriose specialiais reglamentais aiškiai leidžiama tokia trumpalaikė skolinimo praktika pagal priimtas

teisines nuostatas. Tokiais retais atvejais išimtys bus vertinamos pagal taikomus vietos įstatymus ir reguliuojamąsias gaires konkrečioje šalyje.

Turime sugebėti nustatyti ryšį tarp jūsų kūrėjo paskyros ir visų pateiktų licencijų ar dokumentų, įrodančių jūsų gebėjimą teikti asmenines paskolas. Siekiant patvirtinti, kad jūsų paskyra atitinka visus vietos įstatymus ir kitus teisės aktus, gali būti paprašyta papildomos informacijos ar dokumentų.

Asmeninių paskolų programoms arba programoms, kurių pagrindinis tikslas – padėti gauti asmenines paskolas (pvz., potencialių klientų generavimo ir lengvinančioms programoms), papildomoms paskolų programoms (paskolų skaičiuotuvams, paskolų vadovams ir kt.) ir išankstinės prieigos prie uždirbto atlyginimo dalies (angl. „Earned Wage Access“, EWA) programoms draudžiama gauti prieigą prie neskelbtinų duomenų, pavyzdžiui, nuotraukų ir kontaktų. Toliau nurodyti draudžiami leidimai.

- Read_external_storage
- Read_media_images
- Read_contacts
- Access_fine_location
- Read_phone_numbers
- Read_media_videos
- Query_all_packages
- Write_external_storage

Programoms, kuriose naudojama neskelbtina informacija ar API, taikomi papildomi apribojimai ir reikalavimai. Jei reikia papildomos informacijos, žr. [leidimų politiką](#).

Asmeninės paskolos su didele metine palūkanų norma

Jungtinėse Valstijose neleidžiame teikti programų, kuriose teikiamos asmeninės paskolos su 36 % arba didesne metine palūkanų norma (MPN). Jungtinėse Valstijose asmeninėms paskoloms skirtose programose turi būti nurodyta didžiausia MPN, apskaičiuota pagal aktą „[Truth in Lending Act](#)“ (TILA).

Ši politika taikoma programoms, kurios teikia paskolas tiesiogiai, potencialių klientų generavimo programoms ir programoms, kurios klientams padeda susisiekti su trečiosios šalies kreditoriais.

Konkrečios šalies reikalavimai

Pagal nurodytas šalis taikomos asmeninių paskolų programos turi atitikti papildomus reikalavimus ir apibrėžiant finansines funkcijas būtina pateikti papildomų dokumentų sistemoje „[Play Console](#)“. Gavę „Google Play“ užklausą, privalote pateikti papildomos informacijos ar dokumentus, susijusius su jūsų atitiktimi taikomiems reguliavimo ir licencijavimo reikalavimams.

1. Indija

- Jei turite Indijos rezervų banko (IRB) licenciją teikti asmenines paskolas, turite pateikti licencijos kopiją mums peržiūrėti.
- Jei esate netiesiogiai įsitraukę į pinigų skolinimo veiklą ir teikiate tik platformą, kurioje registruotos nebankinių finansinių paslaugų įmonės (NBFC) ar bankai gali skolinti pinigus naudotojams, jums reikia tiksliai paaiškinti tai deklaracijoje.
 - Be to, programos apraše būtina aiškiai paskelbti visų registruotų NBFC ir bankų pavadinimus.

2. Indonezija

- Jei jūsų programa susijusi su informacinėmis technologijomis pagrįstomis pinigų skolinimo paslaugomis, teikiamomis vadovaujantis OJK reglamentu Nr. 77/POJK.01/2016 (kuris retkarčiais gali būti pataisytas), turite pateikti peržiūrėti galiojančios licencijos kopiją.

3. Filipinai

- Visos finansų ir skolinimo įmonės, teikiančios paskolas per internetines skolinimo platformas (angl. „Online Lending Platforms“, OLP), turi gauti SEC registracijos numerį ir įgaliojimo sertifikatą (angl.

„Certificate of Authority“, CA) numerį iš Filipinų vertybinių popierių ir valiutos kursų komisijos (angl. „Philippines Securities and Exchanges Commission“, PSEC).

- Be to, programos apraše turite paskelbti savo korporacijos pavadinimą, įmonės pavadinimą, PSEC registracijos numerį ir įgaliojimo valdyti finansų ir (arba) skolinimo įmonę sertifikatą (CA).
- Programos, susijusios su skolinimu pagrįsto sutelktinio finansavimo veikla, pvz., lygiarangiu (P2P) skolinimu, arba kaip apibrėžta sutelktinį finansavimą reglamentuojančiose taisyklėse ir nuostatuose (CF (angl. „crowdfunding“) taisyklėse), operacijas turi apdoroti per PSEC registruotus CF tarpininkus.

4. Nigerija

- Skaitmeninių pinigų skolinėjai (angl. „Digital Money Lenders“, DML) privalo laikytis Nigerijos Federalinės konkurencijos ir vartotojų apsaugos komisijos (angl. „Federal Competition and Consumer Protection Commission“, FCCPC) nustatytos 2022 m. RIBOTOS LAIKINOSIOS SKAITMENINIŲ PINIGŲ REGULIAVIMO IR (ARBA) REGISTRACIJOS SISTEMOS IR SKOLINIMO GAIRIŲ (su galimais vėlesniais pakeitimais) ir iš FCCPC gauti patikrinamą patvirtinimo raštą.
- Paskolų rinkėjai turite pateikti skaitmeninių skolinimo paslaugų dokumentus ir (arba) sertifikatą bei išsamią kiekvieno bendradarbiaujančio DML kontaktinę informaciją.

5. Kenija

- Skaitmeninių kreditų teikėjai (angl. „Digital Credit Providers“, DCP) turėtų atlikti DCP registracijos procesą ir gauti Kenijos centrinio banko (angl. „Central Bank of Kenya“, CBK) licenciją. Kartu su deklaracija turite pateikti CBK išduotos licencijos kopiją.
- Jei į pinigų skolinimo veiklą esate įsitraukę netiesiogiai ir tik teikiate platformą, kurioje registruoti skaitmeninių kreditų teikėjai gali skolinti pinigus naudotojams, turite tiksliai tai paaiškinti deklaracijoje ir pateikti savo atitinkamo (-ų) partnerio (-ių) DCP licencijos kopiją.
- Šiuo metu priimame deklaracijas ir licencijas tik iš subjektų, paskelbtų Skaitmeninių kreditų teikėjų kataloge oficialioje CBK svetainėje.

6. Pakistanas

- Kiekvienas nebankinių finansinių paslaugų įmonės kreditorius gali skelbti tik vieną skaitmeninio skolinimo programą. Kūrėjai, kurie bando paskelbti daugiau nei vieną nebankinių finansinių paslaugų įmonės skaitmeninio skolinimo programą, kūrėjo ir kitų susijusių paskyrų teikimas gali būti nutrauktas.
- Kad galėtumėte siūlyti ar palengvinti skaitmeninio skolinimo paslaugas Pakistane, turite pateikti Pakistano vertybinių popierių ir valiutos kursų komisijos (angl. „Securities and Exchange Commission of Pakistan“) patvirtinimo įrodymą.

7. Tailandas

- Teikiant asmeninių paslaugų programas, taikomas pagal Tailandą, kai palūkanų norma ne mažesnė kaip penkiolika procentų, būtina gauti galiojančią licenciją iš Tailando banko (angl. „Bank of Thailand“, „BoT“) arba Finansų ministerijos (angl. „Ministry of Finance“, „MoF“). Kūrėjai turi pateikti dokumentus, patvirtinančius, jog jie gali teikti ar padėti gauti asmenines paskolas Tailande. Į šiuos dokumentus turi būti įtraukta:
 - Tailando banko išduotos licencijos vykdyti asmeninių paskolų teikėjo ar „Nano“ finansų organizacijos veiklą, kopija;
 - Finansų ministerijos išduotos „Pico“ finansų verslo licencijos vykdyti „Pico“ ar „Pico-plus“ skolinimo veiklą, kopija.

Toliau pateiktas dažnai pasitaikančio pažeidimo pavyzdys.

Lošimas iš tikrų pinigų, žaidimai ir konkursai

Leidžiame lošimo iš tikrų pinigų programas, skelbimus, susijusius su lošimu iš tikrų pinigų, lojalumo programas su sužaidybintais rezultatais ir kasdienio virtualiojo sporto programas, atitinkančias tam tikrus reikalavimus.

Lošimo programos

Atsižvelgdami į visų „Google Play“ politikos nuostatų apribojimus ir atitiktį, leidžiame programas, kuriose įgalinamas ar skatinamas lošimas internete tam tikrose šalyse, jei kūrėjas [atlieka paraiškos teikimo procesą](#) dėl lošimo programų, platinamų sistemoje „Google Play“, yra patvirtintas valstybinis operatorius ir (arba) yra registruotas kaip licencijuotas operatorius, turintis atitinkamą valstybinių įstaigų išduotą lošimo licenciją atitinkamoje šalyje, ir pateikia galiojančią veiklos licenciją nurodytoje šalyje pagal norimo reklamuoti produkto internetinio lošimo tipą.

Leidžiame tik tokias galiojančias licencijuotas arba įgaliotąsias lošimo programas, kuriose reklamuojami toliau nurodytų tipų internetinio lošimo produktai.

- Internetiniai kazino žaidimai
- Sporto lažybos
- Žirgų lenktynės (kurios reguliuojamos ir licencijuojamos atskirai nuo sporto lažybų)
- Loterijos
- Kasdienis virtualusis sportas

Šios programos turi atitikti toliau nurodytus reikalavimus.

- Kad programą būtų galima platinti per „Google Play“, jos kūrėjas turi sėkmingai [užpildyti paraišką](#).
- Programa turi atitikti visus taikomus įstatymus ir pramonės standartus visose šalyse, kuriose ji platinama.
- Kūrėjas turi turėti galiojančią lošimo licenciją visose šalyse, valstijose ar teritorijose, kuriose platinama programa.

- Kūrėjas negali siūlyti lošimo produktų, kuriems lošimo licencija negalioja.
- Nepilnamečiams naudotojams negali būti leidžiama naudoti programos.
- Programos neturi būti leidžiama pasiekti ir naudoti šalyse, valstijose, teritorijose arba geografinėse vietovėse, kurioms netaikoma kūrėjo lošimo licencija.
- Programos NEGALI būti leidžiama įsigyti kaip mokamos programos sistemoje „Google Play“ ar perkant programoje atsiskaitant per „Google Play“.
- Programą turi būti leidžiama atsisiųsti ir įdiegti iš „Google Play“ parduotuvės be piniginių mokėjimų.
- Programa turi būti įvertinta AO („Adult Only“, liet. „Tik suaugusiems“) arba [atitinkamu IARC įvertinimu](#).
- Programoje ir jos įrašė turi būti aiškiai pateikta informacija apie atsakingą lošimą.

Kitos žaidimų, kuriuose žaidžiama iš tikrų pinigų, konkursų ir turnyrų programos

Visose kitose programose, kurios neatitinka anksčiau minėtų lošimo programų tinkamumo reikalavimų ir nėra įtrauktos į toliau nurodytas kitų žaidimų iš tikrų pinigų bandomąsias programas, neleidžiame teikti turinio ar paslaugų, naudotojams įgalinančių ar palengvinančių lažybas, statymus ar dalyvavimą naudojant tikrus pinigus (įskaitant elementus programoje, įsigijamus už pinigus), kad gautų realios piniginių vertės prizą. Tai apima (bet tuo neapsiribojama) internetinius kazino, sporto lažybas, loterijas ir žaidimus, kuriuose priimami pinigai ir siūloma piniginių ar kitų realiai vertingų prizų (išskyrus programas, leidžiamas pagal toliau aprašytus sužaidybintų lojalumo programų reikalavimus).

Pažaidimų pavyzdžiai

- Žaidimai, kuriuose priimami pinigai už galimybę laimėti fizinį ar piniginių prizą.
- Programos, kuriose yra naršymo elementų ar funkcijų (pvz., meniu elementų, skirtukų, mygtukų, [žiniatinklio rodinių](#) ir kt.), teikiamų raginant veikti, lažintis, statyti ar dalyvauti žaidimuose iš tikrų pinigų, konkursuose ar turnyruose, kur naudojami tikri pinigai, pvz., programos, kuriose naudotojai kviečiami lažintis, užsiregistruoti arba dalyvauti turnyre su galimybe laimėti piniginių prizų.
- Programos, kurios priima arba valdo lažybas, valiutą programoje, laimėjimus ar lošimo užstatus ar kuriose gaunama fizinių ar piniginių prizų.

Kitų žaidimų iš tikrų pinigų bandomosios programos

Retkarčiais tam tikruose regionuose galime vykdyti riboto laiko tam tikrų tipų lošimo iš tikrų pinigų bandomąsias programas. Jei reikia išsamios informacijos, peržiūrėkite šį [pagalbos centro](#) puslapį. Internetinių kelių žaidimų bandomoji programa Japonijoje užbaigta 2023 m. liepos 11 d. Nuo 2023 m. liepos 12 d. internetinių kelių žaidimų programas galima teikti sistemoje „Google Play“ visame pasaulyje, laikantis galiojančių įstatymų ir tam tikrų [reikalavimų](#).

Sužaidybintos lojalumo programos

Jei tai leidžiama pagal įstatymus ir netaikomi papildomi lošimo ar žaidimų licencijavimo reikalavimai, leidžiame lojalumo programas, kuriomis naudotojams atlyginama realiais prizais ar piniginių ekvivalentais pagal toliau nurodytus „Play“ parduotuvės tinkamumo reikalavimus.

Taikoma visoms programoms (žaidimams ir ne žaidimams)

- Lojalumo programos ar kitos privilegijos bei premijos turi aiškiai papildyti reikalavimus atitinkančią piniginių operaciją programoje (kai tinkama piniginių operacija turi būti visiškai atskira operacija, siekiant suteikti su lojalumo programa nesusijusių prekių ar paslaugų) ar ją papildyti ir gali nebūti taikomos pirkiniams ar susietos su bet kokiais mainais, kitu atveju jos pažeis lošimo iš tikrų pinigų, žaidimų ir konkursų politikos apribojimus.
- Pvz., jokia tinkamos „Google“ piniginių operacijos dalis gali neatitikti mokesčio ar lažybų, kad būtų galima dalyvauti lojalumo programoje, o tinkama piniginių operacija negali būti vykdoma įsigyjant prekių ar paslaugų už mažesnę nei įprastą kainą.

Taikoma žaidimų programoms

- Lojalumo programos taškų ar premijų su privilegijomis, nuolaidomis arba premijų, susijusių su tinkama pinigine operacija, galima įsigyti ir išpirkti tik pagal fiksuotą koeficientą, kai jis pastebimai nurodomas programoje ir viešai pasiekiamose oficialiose programos taisyklėse, o privilegijomis teikiamos pajamos ar išperkamoji vertė **negali** būti išlošiamos, teikiamos kaip premija ar eksponuojamos pagal žaidimo našumą arba atsitiktinius rezultatus.

Ne žaidimų programoms

- Lojalumo programos taškai ar premijos gali būti susieti su konkurso arba atsitiktiniais rezultatais, jei atitinka toliau nurodytus reikalavimus. Lojalumo programos su privilegijomis, kitos privilegijos ar premijos, susijusios su tinkama pinigine operacija, turi atitikti toliau nurodytus reikalavimus.
 - Paskelbkite oficialias programos taisykles programoje.
 - Programos, kuriose taikomos kintamumo ar atsitiktinumo principu veikiančios premijų suteikimo sistemos: oficialiose programos sąlygose paskelbkite 1) visų atlygio programų teikiamus šansus, kai nustatant premijas naudojamas fiksuotas koeficientas, ir 2) pasirinkimo metodą (pvz., nustatant premijas naudojamas kintamas koeficientas) visoms kitoms panašioms programoms.
 - Oficialiose programos, kurioje siūlomi lošimai, lažybos žirgų lenktynėse ar kitos panašios reklamos, sąlygose nurodykite fiksuotą nugalėtojų skaičių, fiksuotą pradžios terminą ir prizo paskyrimo datą.
 - Programoje ir oficialiose programos sąlygose pastebimai nurodykite visus fiksuotus kaupiamų ir išperkamų lojalumo programos taškų ar premijų koeficientus.

Programos su lojalumo programa tipas	Lojalumo sužaidybinimas ir kintamos premijos	Lojalumo premijos pagal fiksuotą koeficientą ar tvarkaraštį	Būtinios lojalumo programos taisyklės ir nuostatos	Taisyklėse ir nuostatose turi būti atskleidžiami atsitiktinumo principu ar pasirinkimo metodu veikiančios lojalumo programos teikiami šansai
Žaidimas	Neleidžiama	Leidžiama	Būtina	Netaikoma (žaidimų programose negali būti lojalumo programų atsitiktinumo elementų)
Ne žaidimas	Leidžiama	Leidžiama	Būtina	Būtina

Lošimo arba tikrų pinigų žaidimų, konkursų ir turnyrų skelbimai „Google Play“ platinamose programose

Leidžiame teikti programas, kuriose rodomi lošimo, žaidimų iš tikrų pinigų, konkursų ir turnyrų skelbimai, jei jie atitinka toliau nurodytus reikalavimus.

- Programa ir skelbimas (įskaitant reklamuotojus) turi atitikti visus taikomus įstatymus bei pramonės standartus visose vietovėse, kuriose rodomas skelbimas.
- Skelbimas turi atitikti visus taikomus visų reklamuojamų su lošimu susijusių produktų ir paslaugų vietinius skelbimų licencijų reikalavimus.
- Su lošimu susiję skelbimai programoje negali būti rodomi jaunesniems nei 18 m. asmenims.
- Programa neturi būti programos „Skirta šeimai“ dalis.
- Programos tikslinė auditorija negali būti jaunesni nei 18 m. asmenys.
- Jei reklamuojate lošimo programą (kaip apibrėžta anksčiau), nukreipimo puslapyje, reklamuojamos programos įrašė arba programoje turi būti aiškiai pateikta informacija apie atsakingą lošimą.
- Programoje negali būti imituojamo lošimo turinio (pvz., kazino programų socialiniuose tinkluose; programų su virtualiais lošimo automatais).
- Programoje negali būti lošimo ar žaidimų iš tikrų pinigų, loterijos arba turnyrų palaikymo ar partnerystės funkcijų (pvz., lažybų, išmokėjimų, sporto rezultatų, šansų, našumo stebėjimo arba

dalyvavimo lėšų valdymo funkcijų).

- Programos turinyje negalima reklamuoti lošimo ar žaidimų iš tikrų pinigų, loterijų arba turnyrų paslaugų ar į jas nukreipti naudotojų.

Tik programos, atitinkančios visus šiuos skyriuje išdėstytus reikalavimus (kaip apibrėžta anksčiau), gali apimti lošimo arba žaidimų iš tikrų pinigų, loterijų ar turnyrų skelbimus. Priimamos lošimo programos (kaip apibrėžta anksčiau) arba kasdienio virtualiojo sporto programos (kaip apibrėžta toliau), atitinkančios 1–6 iš pirmiau nurodytų reikalavimų, gali apimti lošimo arba žaidimų iš tikrų pinigų, loterijų ar turnyrų skelbimus.

Pažeidimų pavyzdžiai

- Programa, skirta nepilnamečiams naudotojams, kurioje rodomas lošimo paslaugų skelbimas.
- Imituojamas kazino žaidimas, reklamuojantis arba nukreipiantis naudotojus į kazino, kai naudojami tikri pinigai.
- Speciali sporto šansų stebėjimo programa, kurioje integruoti lošimo skelbimai, nukreipiantys į sporto lažybų svetainę.
- Programos, kuriose yra lošimo skelbimų, pažeidžiančių [apgaulingų skelbimų](#) politiką, pvz., skelbimų, kurie naudotojams rodomi kaip mygtukai, piktogramos ar kiti interaktyvūs elementai programoje.

Kasdienio virtualiojo sporto (angl. „Daily Fantasy Sports“, DFS) programos

Kasdienio virtualiojo sporto (angl. „Daily Fantasy Sports“, DFS) programos, kaip apibrėžta galiojančiuose vietos įstatymuose, leidžiame tik tuo atveju, jei jos atitinka toliau nurodytus reikalavimus.

- Programa yra 1) platinama tik Jungtinėse Amerikos Valstijose arba 2) tinkama pagal anksčiau nurodytus lošimo programų reikalavimus ir paraiškos teikimo procesą šalyse už JAV ribų.
- Kad programą būtų galima platinti per „Google Play“, jos kūrėjas turi sėkmingai [užpildyti DFS paraišką](#).
- Programa turi atitikti visus taikomus įstatymus ir pramonės standartus šalyse, kuriose ji platinama.
- Nepilnamečiams naudotojams negali būti leidžiama lažintis ar vykdyti piniginių operacijų naudojant programą.
- Programos NEGALI būti leidžiama įsigyti kaip mokamos programos sistemoje „Google Play“ ar perkant programoje atsiskaitant per „Google Play“.
- Programą turi būti leidžiama nemokamai atsisiųsti iš „Store“ ir įdiegti.
- Programa turi būti įvertinta kaip AO („Adult Only“, liet. „Tik suaugusiesiems“) arba [atitinkamu IARC įvertinimu](#).
- Programoje ir jos įrašė turi būti aiškiai pateikta informacija apie atsakingą lošimą.
- Programa turi atitikti visus taikomus įstatymus ir pramonės standartus bet kurioje JAV valstijoje ar teritorijoje, kurioje ji platinama.
- Kūrėjas turi turėti licenciją, galiojančią kiekvienoje JAV valstijoje ar teritorijoje, kurioje reikalinga kasdienio virtualiojo sporto programų licencija.
- Programos negalima naudoti JAV valstijose ar teritorijose, kuriose kūrėjas neturi reikalingos kasdienio virtualiojo sporto programų licencijos.
- Programos negalima naudoti JAV valstijose ar teritorijose, kuriose kasdienio virtualiojo sporto programos neteisėtos.

Neteisėta veikla

Neleidžiame teikti programų, kurios palengvina ar skatina neteisėtą veiklą.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Nelegalių narkotinių medžiagų pardavimo ar įsigijimo palengvinimas.

- Narkotikų, alkoholio ar tabako naudojimo ar pardavimo nepilnamečiams vaizdavimas ar skatinimas.
 - Nelegalių vaistų auginimo ar gamybos instrukcijos.
-

Naudotojų sukurtas turinys

Naudotojų sukurtas turinys (NST) – tai turinys, kurį naudotojai pateikia programoje ir kurį gali peržiūrėti ar pasiekti bent dalis programos naudotojų.

Programose, kuriose yra NST, įskaitant programas, kurios yra specializuotos naršyklės arba klientų programos, skirtos nukreipti naudotojus į NST platformą, turi būti tinkamai, veiksmingai ir pastoviai prižiūrimas NST imantis toliau nurodytų priemonių.

- Reikalaujama, kad naudotojai sutiktų su programos naudojimo sąlygomis ir (arba) naudotojo politika, prieš naudotojams kuriant ar įkeliant NST.
- Apibrėžiamas nepriimtinas turinys ir veiksmai (taip, kad jie atitiktų „Google Play“ kūrėjų programos politiką) ir draudžiama juos naudoti programos naudojimo sąlygose ar naudotojo politikoje.
- NST prižiūrimas pagal poreikį ir atsižvelgiant į programoje priglobiamo NST tipą. Tai apima sistemos programoje teikimą, kad būtų galima pranešti apie nepriimtina NST ir naudotojus bei juos blokuoti ir imtis atitinkamų veiksmų dėl NST ar naudotojų. Teikiant skirtingas NST funkcijas gali reikėti skirtingų priežiūros priemonių. Pavyzdys
 - Programose, kuriose yra NST, identifikuojančio nurodytą naudotojų grupę naudojant tokias priemones kaip naudotojų patvirtinimas ar registracija nepriisijungus (pvz., programose, kurios naudojamos tik konkrečioje mokykloje ar įmonėje, ir pan.), turi būti teikiamos pranešimo apie turinį ir naudotojus funkcijos programoje.
 - Naudojant NST funkcijas, įgalinančias individualią naudotojo sąveiką su konkrečiais naudotojais (pvz., tiesioginių pranešimų, žymėjimo, minėjimo ir kitas funkcijas), būtina pateikti naudotojų blokavimo funkcijas programoje.
 - Programose, kuriose teikiama prieiga prie viešai pasiekiamo NST, pvz., socialinių tinklų ir tinklaraštininkų programose, turi būti įdiegtos pranešimo apie naudotojus ir turinį bei naudotojų blokavimo funkcijos programoje.
 - Naudojant išplėtosios realybės (AR) programas, NST tvarkymo funkcija (įskaitant ataskaitų teikimo programoje sistemą) turi apimti ir nepriimtina AR NST (pvz., seksualinio pobūdžio AR vaizdą), ir neskelbtiną AR prieraišo vietą (pvz., AR turinį, kuris susietas su ribojama teritorija, pvz., karine baze arba privačia nuosavybe, kurioje AR prieraišas gali sukelti problemų nuosavybės savininkui).
- Teikiamos apsaugos priemonės, siekiant išvengti pajamų gavimo programoje skatinant nepriimtina naudotojų elgseną.

Atsitiktinis seksualinis turinys

Seksualinis turinys laikomas atsitiktiniu, jei jis rodomas NST programoje, kurioje 1. teikiama prieiga prie pradinio ne seksualinio turinio ir 2. nėra aktyviai reklamuojamas ar rekomenduojamas seksualinis turinys. Seksualinis turinys, kuris galiojančių įstatymų apibrėžiamas kaip neteisėtas, ir [pavojų vaikams](#) keliantis turinys nėra laikomas atsitiktiniu ir nėra leidžiamas.

NST programose gali būti atsitiktinio seksualinio turinio, jei įvykdomi visi toliau nurodyti reikalavimai.

- Toks turinys pagal numatytuosius nustatymus slepiamas, taikant filtrus, kuriuos norėdamas visiškai išjungti naudotojas turi atlikti bent du veiksmus (pavyzdžiui, rodant klaidinantį tarpinį puslapį ar neleidžiant rodyti pagal numatytuosius nustatymus, nebent išjungiama saugi paieška).
- Vaikams, kaip apibrėžta [šeimos politikoje](#), aiškiai draudžiama pasiekti programą, naudojant amžiaus tikrinimo sistemas, pvz., [amžiaus filtrą](#), arba atitinkamą sistemą, apibrėžtą pagal galiojančius įstatymus.
- Programoje pateikiami tikslūs turinio įvertinimo anketos, susijusios su NST, atsakymai, kaip reikalaujama pagal [turinio įvertinimo politiką](#).

Programos, kurių pagrindinis tikslas teikti nepriimtina NST, bus pašalintos iš „Google Play“. Atitinkamai, nustatys, kad programos daugiausia naudojamos nepriimtina NST priglombi arba yra žinomos naudotojams kaip vieta, kurioje galima teikti tokį turinį, šios programos taip pat bus pašalintos iš „Google Play“.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Naudotojų sukurtą seksualinio pobūdžio turinio reklamavimas, įskaitant mokamų funkcijų, kuriomis iš esmės skatinamas nepriimtino turinio bendrinimas, diegimą ar leidimą.
 - Programos su naudotojų sukurtu turiniu (NST), kuriose nepakanka saugos priemonių prieš grąsinimus, priekabiavimą ar patyčias, ypač nukreiptas prieš nepilnamečius.
 - Programoje esantys įrašai, komentarai ar nuotraukos, kurių pirminis tikslas yra priekabiauoti prie kito žmogaus ar išskirti jį iš kitų siekiant piktnaudžiauti, pakenkti ar išjuokti.
 - Programos, kuriose nuolat nepavyksta išspręsti naudotojų skundų dėl nepriimtino turinio.
-

Su sveikata susijęs turinys ir paslaugos

Neleidžiame programų, kuriose naudotojams teikiamas žalingas su sveikata susijęs turinys ir paslaugos.

Jei jūsų programoje yra su sveikata susijusio turinio ir paslaugų arba reklamuojamas toks turinys ir paslaugos, turite užtikrinti, kad programa atitinka visus galiojančius įstatymus ir nuostatas.

Sveikatos programos

Jei jūsų programa yra [sveikatos programa](#) arba joje teikiamos su sveikata susijusios funkcijos ir ji pasiekia sveikatos duomenis, ji turi atitikti taikomą „Google Play“ politiką programų kūrėjams, įskaitant [privatumo](#), [apgaulės ir piktnaudžiavimo įrenginių politiką](#), visuomenę jaudinančių įvykių politiką bei toliau nurodytus reikalavimus.

- **„Console“ deklaracija**
 - Eikite į puslapį „Programos turinys“ („Politika“ > „Programos turinys“) sistemoje „Play Console“ ir pasirinkite kategoriją (-as), kuriai (-ioms) priklauso jūsų programa.
- **Privatumo politika ir aiškaus paskelbimo reikalavimai**
 - Programos privatumo politikos nuoroda turi būti paskelbta atitinkamame sistemos „Play Console“ lauke bei pačioje programoje turi būti paskelbta privatumo politikos nuoroda arba tekstas. Įsitinkite, kad privatumo politika pasiekama aktyviu, viešai pasiekiamu ir pagal geografinę sritį nenustatomu URL adresu (jokių PDF) ir kad jos negalima redaguoti (vadovaujantis [skiltyje „Duomenų sauga“](#) pateiktais reikalavimais).
 - Programos privatumo politikoje kartu su kitais paskelbimais programoje turi būti išsamiai paskelbta, kaip pasiekiami, renkami, naudojami ir bendrinami [asmens ar neskelbtini naudotojų duomenys](#), neapsiribojant duomenimis, paskelbtais anksčiau pateiktoje skiltyje „Duomenų sauga“. Jei naudojamos funkcijos ar duomenys, kurie reguliuojami [pavojingais arba vykdymo laiko leidimais](#), programa turi atitikti visus taikomus [aiškaus paskelbimo ir sutikimo reikalavimus](#).
 - Negalima teikti užklausų dėl leidimų, kurie nėra būtini, kad sveikatos programa galėtų vykdyti pagrindines savo funkcijas, o nenaudojami leidimai turi būti pašalinti. Leidimų, kurie taikomi norint naudoti su sveikata susijusius neskelbtinus duomenis, sąrašą žr. straipsnyje [„Sveikatos programų kategorijos ir papildoma informacija“](#).
 - Jei jūsų programa iš esmės nėra sveikatos programa, bet joje teikiama su sveikata susijusių funkcijų ir pasiekiami sveikatos duomenys, jai vis tiek taikoma sveikatos programos politika. Naudotojas turi aiškiai suprasti ryšį tarp pagrindinių programos funkcijų ir su sveikata susijusių duomenų rinkimo (pvz., draudimo teikėjai, žaidimų programos, kuriose renkami naudotojo veiklos duomenys, siekiant patobulinti žaidimą, ir pan.). Toks ribotas naudojimas turi atsispindėti programos privatumo politikoje.

• Papildomi reikalavimai

Jei jūsų sveikatos programą galima priskirti vienai iš toliau nurodytų kategorijų, turite ne tik sistemoje „Play Console“ pasirinkti tinkamą kategoriją, bet ir atitikti tos kategorijos reikalavimus.

- **Su valdžios institucijomis susijusios sveikatos programos:** jei turite valdžios institucijų ar pripažintos sveikatos priežiūros organizacijos leidimą kurti ir platinti su jomis susijusią programą, turite pateikti tinkamumo reikalavimų įrodymą naudodami [išankstinio pranešimo formą](#).
- **Kontaktų su sergančiais asmenimis išaiškinimo ir (arba) sveikatos būklės programos:** jei jūsų programa yra kontaktų su sergančiais asmenimis išaiškinimo ir (arba) sveikatos būklės programa, sistemoje „Play Console“ pasirinkite „Ligų prevencija ir visuomenės sveikata“ ir anksčiau pateiktoje išankstinio pranešimo formoje nurodykite prašomą informaciją.
- **Su žmonėmis susijusių tyrimų programos:** programose, kuriose atliekami su sveikata susiję žmonių tyrimai, turi būti laikomasi visų taisyklių ir reglamentų, įskaitant (bet neapsiribojant) informuoto dalyvių arba jų tėvų ar globėjų, jei dalyviai nepilnamečiai asmenys, sutikimo gavimą. Be to, sveikatos tyrimų programoms reikia gauti Institucijų peržiūros valdybos (angl. „Institutional Review Board“, IRB) ir (arba) atitinkamo nepriklausomo etikos komiteto patvirtinimą, nebent taikoma išimtis. Gavus užklausą būtina pateikti tokio patvirtinimo įrodymą.
- **Medicinos įrenginių arba programinės įrangos kaip medicinos įrenginio („SaMD“) programos:** naudojant programas, kurios laikomos medicinos įrenginių ar programinės įrangos kaip medicinos įrenginių programomis, būtina gauti ir saugoti leidimo raštą ar kitą patvirtinimo dokumentą, kurį suteikė priežiūros institucija ar subjektas, atsakingi už sveikatos programos valdymą ir reikalavimų laikymąsi. Gavus užklausą būtina pateikti tokio leidimo ar patvirtinimo įrodymą.

„Health Connect“ duomenys

Duomenys, pasiekiami naudojant „Health Connect“ leidimus, laikomi naudotojo asmens ir neskelbtiniais duomenimis, vadovaujantis [Naudotojo duomenų](#) politika ir toliau pateiktais [papildomais reikalavimais](#).

Receptiniai vaistai

Neleidžiame programų, kuriose skatinamas receptinių vaistų pardavimas ar įsigijimas be recepto.

Nepatvirtintos medžiagos

Sistemoje „Google Play“ neleidžiamos programos, kuriose reklamuojamos ar parduodamos nepatvirtintos medžiagos, neatsižvelgiant į jokių tvirtinimų dėl jų teisėtumo.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Visi elementai, įtraukti į nebaigtinį [draudžiamų vaistų ir papildų sąrašą](#).
- Produktai, kurių sudėtyje yra efedros.
- Produktai, kurių sudėtyje yra žmogaus chorioninio gonadotropino (hCG) ir kurie reklamuojami kartu su anaboliniais steroidais arba siūlant numesti svorio ar jį reguliuoti.
- Žolelių ir dietiniai papildai, kurių sudėtyje yra aktyviųjų vaistinių ar pavojingų medžiagų.
- Melagingi arba klaidinantys su sveikatos priežiūra susiję tvirtinimai, įskaitant tvirtinimus, kad produktas yra toks pat veiksmingas kaip ir receptiniai vaistai ar medžiagos, kurių naudojimas kontroliuojamas.
- Valstybės institucijų nepatvirtinti produktai, kurie pateikiami rinkai taip, tarsi jie būtų saugūs arba efektyvūs, siekiant apsaugoti nuo tam tikrų ligų ir negalavimų arba gydant nuo jų.
- Produktai, dėl kurių buvo perspėta arba imtasi bet kokių vyriausybės ar teisinių veiksmų.
- Produktai, kurių pavadinimai klaidingai panašūs į nepatvirtintų vaistų, papildų ar medžiagų, kurių naudojimas kontroliuojamas, pavadinimus.

Jei reikia papildomos informacijos apie mūsų kontroliuojamus nepatvirtintus ar klaidinančių pavadinimų vaistus ir papildus, apsilankykite adresu www.legitscript.com.

Klaidinga su sveikata susijusi informacija

Neleidžiame programų, kuriose yra nepagrįstų su sveikatos priežiūra susijusių tvirtinimų, prieštaraujančių esamam medicininiam sutarimui ar galinčių pakenkti naudotojams.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Nepagrįsti tvirtinimai apie vakcinas, pvz., teiginiai, kad vakcinos gali pakeisti asmens DNR.
- Žalingo, nepatvirtinto gydymo propagavimas.
- Kitų žalingų su sveikata susijusių metodų, pvz., konversijos terapijos, propagavimas.

Su medicina susijusios funkcijos

Neleidžiame teikti programų, apimančių su medicina ar sveikata susijusias funkcijas, kurios yra klaidinančios ar potencialiai žalingos. Pvz., neleidžiame programų, kuriose tvirtinama, kad teikiamos oksimetro funkcijos, pagrįstos tik programa. Oksimetro programos turi būti palaikomos išorinės aparatinės įrangos, nešiojamųjų įrenginių ar tam tikrų išmaniųjų telefonų jutiklių, skirtų oksimetro funkcijoms palaikyti. Be to, šių palaikomų programų metaduomenyse turi būti pateiktas atsisakymas, kuriame turi būti nurodyta, kad programa nėra skirta naudoti medicinos tikslais, naudojama tik bendrojo pobūdžio kūno rengybos ir sveikatinimo tikslais, tai nėra medicinos įrenginys, bei turi būti tinkamai pateiktas suderinamos aparatinės įrangos ir (arba) įrenginio modelis.

Mokėjimai – klinikinės paslaugos

Atliekant operacijas, apimančias kontroliuojamas klinikinės paslaugas, „Google Play“ atsiskaitymo sistemų naudoti nereikia. Jei reikia daugiau informacijos, žr. straipsnį [„Google Play“ mokėjimų politikos paaiškinimas](#).

Blokų grandine pagrįstas turinys

Sparčiai tobulėjant blokų grandinių technologijoms stengiamės teikti kūrėjams platformą, kur jie galėtų pasitelkti naujoves ir kurti geresnes, labiau įtraukiančias funkcijas naudotojams.

Pagal šią politiką blokų grandinių turinys laikomas skaitmeniniais ištekliais su prieigos raktais, kurie saugomi blokų grandinėje. Jei jūsų programoje yra blokų grandinių turinio, turite laikytis šių reikalavimų.

Kripto valiutos keityklos ir programinės piniginės

Kripto valiutos įsigijimo, laikymo ar keitimo paslaugas turėtų teikti sertifikuotos tarnybos reguliuojamose jurisdikcijose.

Be to, privalote laikytis regione ar šalyje, kuriuose taikoma jūsų programa, galiojančių reglamentų ir neskelbti programos, kur jūsų produktai ir paslaugos draudžiami. „Google Play“ gali paprašyti pateikti papildomos informacijos ar dokumentų, susijusių su galiojančių reguliavimo ar licencijavimo reikalavimų laikymusi.

Kripto valiutos kasimas

Neleidžiame teikti programų, kuriomis įrenginiuose išgaunama kripto valiuta. Leidžiame teikti programas, kuriomis nuotoliniu būtu valdoma kripto valiutos gavyba.

Skaitmeninių išteklių su prieigos raktais platinimo skaidrumo reikalavimai

Jeigu jūsų programoje parduodami skaitmeniniai ištekliai su prieigos raktais arba suteikiama galimybė naudotojams juos gauti, turite tai apibrėžti finansinių funkcijų deklaracijos formoje programos turinio puslapyje sistemoje „Play Console“.

Kurdami produktą programoje išsamioje produkto informacijoje turite nurodyti, kad tai yra skaitmeninis išteklius su prieigos raktu. Jei reikia daugiau gairių, žr. skiltį „[Produkto programoje kūrimas](#)“.

Negalite reklamuoti ar skatinti gauti jokių potencialių pajamų iš žaidimo ar prekybos veiklos.

Papildomi NFT sužaidybinių reikalavimai

Vadovaujantis „Google Play“ [lošimo iš tikrų pinigų, žaidimų ir konkursų politika](#), lošimo programos, kuriose integruota skaitmeninių išteklių su prieigos raktais, pvz., NFT, turi atitikti paraiškos proceso reikalavimus.

Visose kitose programose, kurios neatitinka lošimo programų tinkamumo reikalavimų ir nėra įtrauktos į [kitų žaidimų iš tikrų pinigų bandomąsias programas](#), jokie piniginės vertės elementai negali būti priimami, kad būtų suteikta galimybė gauti nežinomos vertės NFT. Naudotojų įsigyti NFT turi būti apdorojami ar naudojami žaidime naudotojo patirčiai pagerinti ir padėti naudotojams pasiekti aukštesnį žaidimo lygį. NFT negali būti naudojami lažyboms ar statymams, kad būtų suteikta galimybė laimėti realios piniginės vertės prizų (įskaitant kitus NFT).

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Programos, kuriose parduodami NFT rinkiniai neatskleidžiant konkretaus NFT turinio ir vertės.
- Mokami kazino žaidimai socialiniuose tinkluose, pvz., lošimo automatai, kur galima gauti NFT.

DI sugeneruotas turinys

Kadangi generatyvinio DI modeliai tampa vis plačiau pasiekiami kūrėjams, galite įtraukti šiuos modelius į programas, kad padidintumėte naudotojų įtraukimą ir pagerintumėte jų patirtį. „Google Play“ nori padėti užtikrinti, kad DI sugeneruotas turinys yra saugus visiems naudotojams ir kad atsižvelgiama į naudotojų atsiliepimus kuriant patikimas naujoves.

DI sugeneruotas turinys

DI sugeneruotas turinys – tai turinys, sukurtas naudojant generatyvinio DI modelius pagal naudotojų klausimus. DI sugeneruoto turinio pavyzdžiai

- Teksto pokalbių generatyvinio DI pokalbių robotai, kai sąveika su pokalbių robotu yra pagrindinė programos funkcija.
- DI sugeneruotas vaizdas pagal teksto, vaizdo ar balso užklausas.

Siekiant užtikrinti naudotojų saugą ir atsižvelgiant į „Google Play“ [politikos aprėptį](#), programos, kuriose turinys generuojamas naudojant DI, turi atitikti esamą „Google Play“ politiką programų kūrėjams, įskaitant draudimą generuoti [apribotą turinį](#), pvz., [turinį, skatinantį vaikų išnaudojimą ar prievartą](#), ir [apgaulingą elgseną](#) įgalinantį turinį, bei tokio turinio prevenciją.

Programose, kuriose generuojamas turinys naudojant DI, turi būti naudotojams teikiamos pranešimo ar žymėjimo funkcijos programoje, leidžiančios naudotojams pažymėti ar pranešti apie įžeidžiantį turinį kūrėjams, neišėjus iš programos. Atsižvelgdami į naudotojų pranešimus kūrėjai turėtų koreguoti turinio filtravimą ir moderavimą programose.

Intelektinė nuosavybė

Neleidžiame teikti programų ar naudoti kūrėjų paskyrų, kuriose pažeidžiamos kitų intelektinės nuosavybės teisės (įskaitant prekių ženklų, autorių teisių, patentų, komercinių paslapčių ir kitas firmines teises). Be to, neleidžiame teikti programų, kuriose skatinama pažeisti intelektinės nuosavybės teises.

Reaguosime į aiškius pranešimus apie tariamus autorių teisių pažeidimus. Jei reikia daugiau informacijos arba norite pateikti DMCA užklausą, žr. [autorių teisių procedūras](#) .

Jei norite pateikti skundą dėl suklastotų prekių pardavimo ar reklamos programoje, pateikite [pranešimą apie klastojimą](#) .

Jei esate prekės ženklo savininkas ir manote, kad „Google Play“ pateikiama jūsų prekės ženklo teisės pažeidžianti programa, raginame susisiekti tiesiogiai su kūrėju ir išspręsti problemą. Jei nepavyksta išspręsti problemos su kūrėju, pateikite skundą dėl prekės ženklo naudojimo, užpildydami šią [formą](#) .

Jei turite rašytinių dokumentų, įrodančių, kad turite leidimą programoje arba parduotuvės įrašė naudoti trečiosios šalies intelektinę nuosavybę (pvz., prekių ženklų pavadinimus, logotipus ir grafinius išteklius), prieš pateikdami [susisiekite su „Google Play“ komanda](#) , kad programa nebūtų atmesta dėl intelektinės nuosavybės pažeidimo.

Neteisėtas autorių teisių saugomo turinio naudojimas

Neleidžiame teikti autorių teises pažeidžiančių programų. Pakeitus autorių teisių saugomą turinį teisės vis tiek gali būti pažeidžiamos. Kūrėjams gali reikėti pateikti įrodymų apie turimas teises naudoti autorių teisių saugomą turinį.

Pristatydami programos funkcijas, autorių teisių saugomą turinį naudokite atsargiai. Apskritai saugiausia sukurti kažką originalaus.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

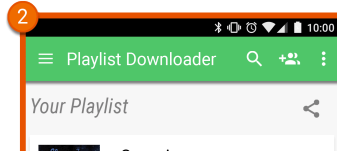
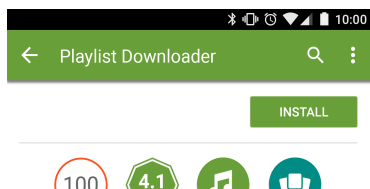
- Muzikos albumų, vaizdo žaidimų ir knygų viršelių vaizdai.
- Rinkodaros vaizdai iš filmų, televizijos ar vaizdo žaidimų.
- Plakatai ar vaizdai iš komiksų knygų, animacinių filmų, filmų, muzikinių vaizdo įrašų ar televizijos laidų.
- Koledžo ir profesionalių sporto komandų logotipai.
- Nuotraukos iš viešo asmens visuomeninės medijos paskyros.
- Profesionalios viešų asmenų nuotraukos.
- Kopijos ar „gerbėjų meno“ kūriniai, kuriuos sunku atskirti nuo originalaus autorių teisių saugomo kūrinio.
- Programos, kuriose grojami garso įrašai iš autorių teisių saugomo turinio.
- Ne viešajame domene esančių knygų kopijos ar vertimai.

Autorių teisių pažeidimo skatinimas

Neleidžiame teikti programų, kuriose verčiama arba skatinama pažeisti autorių teises. Prieš skelbdami savo programą peržiūrėkite, ar joje neskatinama pažeisti autorių teisių, ir prireikus pasitarkite su teisininku.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Programų, kuriose naudotojams leidžiama atsisiųsti vietinę autorių teisių saugomo turinio kopiją neturint įgaliojimų, perdavimas srautu.
- Programos, kuriose naudotojai skatinami perduoti srautu ir atsisiųsti autorių teisių saugomą turinį, įskaitant muziką ir vaizdo įrašus, taip pažeidžiant taikomą autorių teisių įstatymą.



- ① Šiame programos įrašė pateikiamas aprašas skatina naudotojus atsisiųsti autorių teisių saugomą turinį neturint įgaliojimų.
- ② Programos įrašė esančioje ekrano kopijoje naudotojai skatinami atsisiųsti autorių teisių saugomą turinį neturint įgaliojimų.

Prekių ženklų savininkų teisių pažeidimas

Neleidžiame teikti programų, kurios pažeidžia kitų prekės ženklų savininkų teises. Prekės ženklas – tai žodis, simbolis arba jų derinys, identifikuojantis prekės ar paslaugos šaltinį. Įgijęs prekės ženklą jo savininkas gauna išskirtines teises naudoti jį su atitinkamomis prekėmis ar paslaugomis.

Prekės ženklo savininko teisių pažeidimas ar netinkamas arba neleistas panašaus prekės ženklo naudojimas taip, kad gali kilti abejonių dėl to produkto šaltinio. Jei jūsų programoje naudojami kitos šalies prekių ženklai ir toks naudojimas gali sukelti neaiškumų, jūsų programa gali būti laikinai sustabdyta.

Klastotė

Neleidžiame programų, kuriose parduodamos suklastotos prekės arba reklamuojamas jų pardavimas. Suklastotos prekės žymimos prekių ženklais arba logotipais, kurie yra tokie pat kaip kitų prekių ženklai arba iš esmės nuo jų nesiskiria. Tokiomis prekėmis imituojamos produkto prekės ženklo ypatybės pateikiant jas kaip originalų prekės ženklo savininko produktą.

Privatumas, apgaulė ir piktnaudžiavimas įrenginiu

Stengiamės saugoti naudotojų privatumą ir teikti saugias paslaugas. Apgaulingos, kenkėjiškos programos, kurios piktnaudžiauja tinklu, įrenginiu arba asmeniniais duomenimis arba juos netinkamai naudoja, yra griežtai draudžiamos.

Naudotojo duomenys

Turite aiškiai nurodyti, kaip apdorojate naudotojo duomenis (pvz., iš naudotojo arba apie jį surinktą informaciją, įskaitant įrenginio informaciją). Tai reiškia, kad reikia atskleisti, kaip pasiekiate, renkate, naudojate, tvarkote ir bendrinatė programos naudotojo duomenis, bei apriboti duomenų naudojimą pagal duomenų atskleidimo politikos reikalavimus. Atkreipkite dėmesį, kad tvarkant asmens ir

neskelbtinus naudotojo duomenis, taip pat taikomi papildomi reikalavimai, nurodyti toliau pateiktoje skiltyje „Asmens ir neskelbtini naudotojo duomenys“. Šie „Google Play“ reikalavimai papildo visus taikomuose privatumo ir duomenų apsaugos įstatymuose numatytus reikalavimus.

Jei į programą įtraukiate trečiosios šalies kodą (pvz., SDK), privalote užtikrinti, kad programoje naudojamas trečiosios šalies kodas ir tos trečiosios šalies veiksmai, susiję su programoje esančiais naudotojo duomenimis, atitiktų „Google Play“ kūrėjų programos politiką, įskaitant naudojimo ir atskleidimo reikalavimus. Pavyzdžiui, turite užtikrinti, kad SDK teikėjai neparduotų asmens ir neskelbtinų programos naudotojų duomenų. Šis reikalavimas taikomas neatsižvelgiant į tai, ar naudotojo duomenys perduodami juos nusiuntus į serverį, ar į programą įterpiant trečiosios šalies kodą.

Asmens ir neskelbtini naudotojo duomenys

Asmens ir neskelbtini naudotojo duomenys apima (bet tuo neapsiriboja) asmens identifikavimo informaciją, finansinę ir mokėjimo informaciją, autentifikavimo informaciją, telefonų knygą, kontaktus, [įrenginio vietovę](#) , su SMS ir skambučiais susijusius duomenis, [sveikatos duomenis](#) , „[Health Connect](#)“ duomenis, kitų įrenginio programų skelbimų vietas, mikrofono, fotoaparato ir kitus neskelbtinus įrenginio ar naudojimo duomenis. Jei programoje tvarkomi asmens ir neskelbtini naudotojo duomenys, turite atitikti šiuos reikalavimus:

- iš programos gautus asmens ir neskelbtinus naudotojo duomenis, pasiekti, rinkti, naudoti ir bendrinti tik programos ir paslaugos funkcijų teikimo bei politikos atitikimo tikslais, kurių pagrįstai tikisi naudotojas;
- programos, kuriose asmens ir neskelbtini naudotojo duomenys naudojami reklamai rodyti, turi atitikti „Google Play“ [skelbimų politiką](#) ;
- duomenis prireikus taip pat galite perduoti [paslaugų teikėjams](#) arba dėl teisinių priežasčių, pvz., laikydamiesi galiojančios vyriausybės užklausos, taikomo įstatymo ar vykdydami sujungimo ar įsigijimo procesą, apie tai pranešę naudotojams pagal teisinius reikalavimus;
- saugiai tvarkyti visus asmens ir neskelbtinus naudotojo duomenis, įskaitant jų perdavimą naudojant modernią kriptografiją (pvz., per HTTPS);
- naudoti vykdymo laiko leidimų užklausą (kai pasiekama), prieš pasiekdami duomenis, kuriems taikomi „[Android](#)“ [leidimai](#) ;
- neparduoti asmens ir neskelbtinų naudotojo duomenų.
 - Pardavimas yra keitimasis asmens ir neskelbtiniais naudotojo duomenimis arba jų perdavimas [trečiajai šaliai](#) už piniginį atlygį.
 - Naudotojo inicijuotas asmens ir neskelbtinų naudotojo duomenų perdavimas (pavyzdžiui, kai naudotojas, naudodamas programos funkciją, perduoda failą trečiajai šaliai ar nusprendžia naudoti specialios paskirties mokslinių tyrimų programą) nelaikomas pardavimu.

Aiškaus paskelbimo ir sutikimo reikalavimas

Jei jūsų programos prieiga prie asmens ir neskelbtinų naudotojo duomenų, jų rinkimas, naudojimas ar bendrinimas gali neatitikti pagrįstų atitinkamo produkto ar funkcijos naudotojo lūkesčių (pavyzdžiui, jei duomenys renkami fone, kai naudotojas nesinaudoja programa), privalote laikytis toliau nurodytų reikalavimų.

Aiškus paskelbimas: programoje turite paskelbti apie duomenų pasiekimą, rinkimą, naudojimą ir bendrinimą. Paskelbimas programoje turi atitikti toliau nurodytus reikalavimus.

- Turi būti pačioje programoje, o ne tik programos apraše arba svetainėje.
- Turi būti rodomas įprastai naudojant programą, o ne naudotojui apsilankius meniu ar nustatymuose.
- Jame turi būti aprašyti pasiekiami ar renkami duomenys.
- Turi paaiškinti, kaip bus naudojami ir (arba) bendrinami duomenys.
- Jo negalima įtraukti vien tik į privatumo politiką arba paslaugų teikimo sąlygas.

- Jo negalima pateikti su kitais paskelbimais, nesusijusiais su asmens ir neskelbtinų naudotojo duomenų rinkimu.

Sutikimo ir vykdymo laiko leidimai: programos naudotojo sutikimo ir vykdymo laiko leidimo užklausa turi būti pateiktos iš karto po paskelbimo programoje, atitinkančio šios politikos reikalavimus. Programos sutikimo užklausa turi atitikti toliau nurodytus reikalavimus.

- Turi būti aiškiai, nedviprasmiškai pateikiamas sutikimo dialogo langas.
- Turi būti reikalaujama naudotojo patvirtinamojo veiksmo (pvz., sutikti palietus, pažymėti žymimąjį langelį).
- Negalima patvirtinimu laikyti išėjimo iš paskelbimo lango (įskaitant išėjimą palietus arba mygtuko „Atgal“ ar pagrindinio ekrano mygtuko paspaudimą).
- Negalima naudoti pranešimų, kurių atsisakoma automatiškai arba kurių galiojimas baigiasi, siekiant gauti naudotojo sutikimą.
- Naudotojas sutikimą turi pateikti prieš programai pradėdant rinkti asmens ir neskelbtinus naudotojo duomenis ar juos pasiekiant.

Programos, kurios, tvarkydamos asmens ir neskelbtinus naudotojo duomenis be sutikimo, remiasi kitu teisiniu pagrindu, pvz., teisėtu interesu pagal ES BDAR, privalo laikytis visų taikomų teisinių reikalavimų ir naudotojams pateikti tinkamus atskleidimus, įskaitant atskleidimą programoje, kaip reikalaujama pagal šią politiką.

Toliau pateikiamas aiškaus paskelbimo formato pavyzdys, kuriuo rekomenduojama vadovautis siekiant laikytis politikos reikalavimų.

- „[Ši programa] renka / perduoda / sinchronizuoja / saugo [duomenų tipą], kad būtų galima naudoti [funkciją] [nurodytais atvejais].“
- Pavyzdys: „Fitness Funds“ renka vietovės duomenis, kad būtų galima stebėti mankštą net tada, kai programa uždaryta ar nenaudojama. Duomenys taip pat naudojami reklamavimo palaikymo tikslais.“
- Pavyzdys: „Call Buddy“ renka skaitomus ir rašomus skambučių žurnalo duomenis, kad būtų galima tvarkyti kontaktus net tada, kai programa nenaudojama.“

Jei programoje integruotas trečiosios šalies kodas (pvz., SDK), kuris pagal numatytuosius nustatymus yra skirtas rinkti asmens ir neskelbtinus naudotojo duomenis, per dvi savaites nuo „Google Play“ užklauso gavimo (arba, jei „Google Play“ užklausoje numatytas ilgesnis laikotarpis, per tą laikotarpį) turite pateikti pakankamai įrodymų, kad programa atitinka šios politikos aiškaus paskelbimo ir sutikimo reikalavimus, įskaitant susijusius su prieiga prie duomenų, jų rinkimu, naudojimu ar bendrinimu naudojant trečiosios šalies kodą.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Programa, kuri renka įrenginio vietovės duomenis, bet joje nėra aiškaus paskelbimo, kuriame būtų paaiškinta, kuri funkcija naudoja šiuos duomenis, ir (arba) nurodytas programos naudojimas fone.
- Programa, kuri turi vykdymo laiko leidimą, prašantį suteikti prieigą prie duomenų prieš pateikiant aiškų paskelbimą, kuriame nurodoma, kam naudojami duomenys.
- Programa, kuri pasiekia naudotojo įdiegtų programų skelbimų vietas ir kurioje šie duomenys nelaikomi asmens ar neskelbtiniais duomenimis, kuriems taikomi anksčiau nurodyti privatumo politikos, duomenų apdorojimo ir aiškaus paskelbimo bei sutikimo reikalavimai.
- Programa, kuri pasiekia naudotojo telefono arba kontaktų knygos duomenis ir kurioje šie duomenys nelaikomi asmens ar neskelbtiniais duomenimis, kuriems taikomi anksčiau nurodyti privatumo politikos, duomenų apdorojimo ir aiškaus paskelbimo bei sutikimo reikalavimai.
- Programa, kuri įrašo naudotojo ekrano duomenis ir kurioje šie duomenys nelaikomi asmens ar neskelbtiniais duomenimis, kuriems taikoma ši politika.
- Programa, kurioje renkama [įrenginio vietovės](#) informacija ir išsamiai neskelbiama apie jos naudojimą bei negaunamas sutikimas pagal pirmiau nurodytus reikalavimus.
- Programa, kurioje naudojami riboti leidimai programos fone, įskaitant stebėjimo, tyrimo ar rinkodaros tikslais, ir išsamiai neskelbiama apie jų naudojimą bei negaunamas sutikimas pagal pirmiau

nurodytus reikalavimus.

- Programa su SDK, kuri renka asmens ir neskelbtinus naudotojo duomenis ir šiems duomenims netaiko šios naudotojų duomenų politikos, prieigos, duomenų tvarkymo (įskaitant neleistiną pardavimą) ir aiškaus paskelbimo ir sutikimo reikalavimų.

Jei reikia daugiau informacijos apie aiškaus paskelbimo ir sutikimo reikalavimą, žr. šį [straipsnį](#).

Prieigos prie asmens ir neskelbtinų duomenų apribojimai

Be anksčiau nurodytų reikalavimų, toliau pateiktoje lentelėje aprašomi konkrečiai veiklai taikomi reikalavimai.

Veikla	Reikalavimas
Programa apdoroja finansų ar mokėjimo informaciją arba vyriausybės išduotų tapatybės dokumentų numerius	Programoje jokių būdu negali būti viešai atskleisti jokie asmens ir neskelbtini naudotojų duomenys, susiję su finansų ar mokėjimo veikla arba bet kokiais vyriausybės išduotų tapatybės dokumentų numeriais.
Programa apdoroja neviešą telefonų knygos ar kontaktinę informaciją	Draudžiame neteisėtai skelbti ar atskleisti žmonių neviešą kontaktinę informaciją.
Programoje yra antivirusinių ar saugos funkcijų, pvz., antivirusinių, skirtų kovoti su kenkėjiškomis programomis ar su sauga susijusių funkcijų	Programoje turi būti paskelbta privatumo politika, kurioje, kartu su bet kokiais paskelbimais programoje, būtų paaiškinta, kokius naudotojo duomenis programa renka ir perduoda, kaip jie naudojami ir su kokių tipų šalimis bendrinami.
Programa taikoma vaikams	Programoje negali būti SDK, kuris nepatvirtintas naudoti vaikams skirtose paslaugose. Išsamių politikos nuostatų ir reikalavimų žr. straipsnyje „ Vaikams ir šeimoms skirtų programų kūrimas “.
Programoje renkami arba susiejami nuolatiniai įrenginio identifikatoriai (pvz., IMEI, IMSI, SIM serijos numeris ir pan.)	Nuolatinį įrenginio identifikatorių negalima susieti su kitais asmens ir neskelbtiniais naudotojų duomenimis arba iš naujo nustatomais įrenginio identifikatoriais, išskyrus atvejus, kai tai būtina norint teikti: • telefonijos paslaugas, susietas su SIM kortelės tapatybės nustatymu (pvz., „Wi-Fi“ skambinimo, susieto su operatoriaus paskyra, paslaugas), ir • žmonių įrenginių tvarkymo programas, kuriose naudojamas įrenginio savininko režimas. Apie tokį naudojimą turi būti aiškiai paskelbta naudotojams, kaip nurodyta naudotojo duomenų politikoje. Daugiau informacijos apie alternatyvius unikalius identifikatorius rasite šiame šaltinyje. Norėdami gauti papildomos informacijos apie „Android“ reklamavimo ID, perskaitykite skelbimų politiką.

Skiltis „Duomenų sauga“

Visi kūrėjai turi pateikti aiškią ir tikslią informaciją kiekvienos programos „Duomenų saugos“ skiltyje, kurioje išsamiai apibūdinamas naudotojų duomenų rinkimas, naudojimas ir bendrinimas. Kūrėjas yra atsakingas už privatumo etiketės tikslumą ir joje pateikiamos informacijos atnaujinimą. Jei reikalaujama, skiltyje pateikta informacija turi atitikti programos privatumo politikoje pateiktus paskelbimus.

Jei reikia papildomos informacijos apie skilties „Duomenų sauga“ pildymą, žr. šį [straipsnį](#).

Privatumo politika

Kiekvienos programos privatumo politikos nuoroda turi būti paskelbta atitinkamame sistemos „Play Console“ lauke bei pačioje programoje turi būti paskelbta privatumo politikos nuoroda arba tekstas. Privatumo politikoje kartu su kitais paskelbimais programoje turi būti išsamiai paskelbta, kaip programa

pasiekia, renka, naudoja ir bendrina naudotojų duomenis, neapsiribojant duomenimis, paskelbtais skiltyje „Duomenų sauga“. Tai turi apimti:

- kūrėjo informaciją ir kontaktinio asmens, į kurį galima kreiptis dėl privatumo klausimų, informaciją arba užklausų pateikimo mechanizmą;
- paskelbimą, kokių tipų asmens ir neskelbtinus naudotojų duomenis jūsų programa pasiekia, renka, naudoja ir bendrina bei su kokiais šalimis bendrinami bet kokie asmens ar neskelbtini naudotojų duomenys;
- saugaus asmens ir neskelbtinų naudotojų duomenų tvarkymo procedūras;
- kūrėjo duomenų saugojimo ir ištrynimo politiką;
- aiškų nurodymą, kad tai yra privatumo politika (pvz., pavadinime nurodoma „privatumo politika“).

Subjektas (pvz., kūrėjas, įmonė), nurodytas programos „Google Play“ parduotuvės įrašė, turi būti nurodytas privatumo politikoje arba programa turi būti nurodyta privatumo politikoje. Programose, kuriose nepasiekiami jokių asmens ir neskelbtinų naudotojų duomenų, vis tiek turi būti pateikta privatumo politika.

Įsitikinkite, kad privatumo politika pasiekiami aktyviu, viešai pasiekiamu ir pagal geografinę sritį nenustatomu URL adresu (jokių PDF) ir kad jos negalima redaguoti.

Paskyros ištrynimo reikalavimas

Jei programa leidžia naudotojams sukurti paskyrą programoje, ji taip pat turi leisti naudotojams pateikti užklausą dėl paskyros ištrynimo. Naudotojams turi būti pateikta lengvai aptinkama parinktis inicijuoti programos paskyros ištrynimą programoje ir ne programoje, pvz., apsilankius svetainėje. Šio žiniatinklio šaltinio nuorodą reikia pateikti atitinkamame URL formos lauke sistemoje „Play Console“.

Kai ištrinate programos paskyrą, gavę naudotojo užklausą, taip pat turite ištrinti naudotojo duomenis, susijusius su šios programos paskyra. Laikinas programos paskyros išaktyvinimas, išjungimas ar „užšaldymas“ nelaikomas paskyros ištrynimu. Jei tam tikrus duomenis reikia saugoti teisėtais tikslais, pvz., norint užtikrinti saugą, išvengti apgaulės ar laikytis reguliavimo reikalavimų, turite aiškiai informuoti naudotojus apie duomenų saugojimo praktiką (pavyzdžiui, privatumo politikoje).

Jei norite sužinoti daugiau apie paskyros ištrynimo politikos reikalavimus, perskaitykite šį [pagalbos centro](#) straipsnį. Jei reikia daugiau informacijos apie tai, kaip atnaujinti duomenų saugos formą, skaitykite šį [straipsnį](#).

Nustatyto programos ID naudojimas

Bus pristatyti nauji „Android“ įrenginiams skirti ID, taikytini pagrindiniams naudojimo atvejams, pvz., analitikai ir apsaugai nuo apgaulės. Šių ID naudojimo sąlygos nurodytos toliau.

- **Naudojimas:** nustatytą programos ID negalima naudoti skelbimams suasmeninti ir vertinti.
- **Susiejimas su asmens identifikavimo informacija ar kitais identifikatoriais:** nustatyto programos ID negalima jungti su jokiais kitais „Android“ identifikatoriais (pvz., AAID), asmens ir neskelbtiniais duomenimis, kai tai daroma reklamavimo tikslais.
- **Skaidrumas ir sutikimas:** informacijos rinkimas ir nustatyto programos ID naudojimas bei įsipareigojimas laikytis šių taisyklių turi būti nurodyti naudotojams teisėtame privatumo pranešime, įskaitant jūsų privatumo politiką. Privalote gauti teisiškai galiojantį naudotojų sutikimą, kai jo reikia. Jei norite sužinoti daugiau apie mūsų privatumo standartus, žr. [naudotojų duomenų politiką](#).

„EU-U.S. Privacy Shield“ (ES–JAV privatumo skydas) ir „Swiss Privacy Shield“ (Šveicarijos privatumo skydas)

Jei pasiekiate, naudojate ar apdorojate „Google“ teikiamą asmens informaciją, kuri tiesiogiai ar netiesiogiai identifikuoja asmenį ir kuri buvo pateikta Europos Sąjungoje ar Šveicarijoje („ES asmens informacija“), turite:

- laikytis visų taikomų privatumo, duomenų saugos ir duomenų apsaugos įstatymų, direktyvų, nuostatų ir taisyklių;
- pasiekti, naudoti ar apdoroti ES asmens informaciją tik tais tikslais, kuriais buvo gautas su ta ES asmens informacija susijusio asmens sutikimas;
- taikyti atitinkamas organizacines ir technines priemones, skirtas apsaugoti ES asmens informaciją nuo praradimo, netinkamo naudojimo ir neteisėtos prieigos, atskleidimo, keitimo ir sunaikinimo;
- teikti tokio lygio apsaugą, kokios reikalaujama pagal „Privacy Shield“ (Privatumo skydo) principus .

Turite reguliariai tikrinti, ar atitinkate šias sąlygas. Jei kada nors negalėsite atitikti šių sąlygų (arba jei yra didelė rizika, kad negalėsite jų atitikti), turite nedelsdami pranešti apie tai mums el. paštu data-protection-office@google.com ir iš karto nustoti apdoroti ES asmens informaciją arba atlikti atitinkamus veiksmus, kad atkurtumėte tinkamą apsaugą.

Nuo 2020 m. liepos 16 d. „Google“ nebetaiko „EU-U.S. Privacy Shield“ (ES–JAV privatumo skydo) perkeldama asmens duomenis iš Europos ekonominė erdvės šalių ar JK į JAV. (Sužinokite daugiau.) Daugiau informacijos rasite KPS 9 skirsnyje.

Leidimai ir API, kurie pasiekia neskelbtiną informaciją

Leidimų ir API, kurie pasiekia neskelbtiną informaciją, užklauskos turi būti suprantamos naudotojams. Galite pateikti užklausą tik dėl tų neskelbtiną informaciją pasiekiančių leidimų ir API, kurie yra būtini norint įdiegti esamas programos funkcijas ar paslaugas, reklamuojamas „Google Play“ įrašė. Negalite naudoti leidimų ar API, kurie pasiekia neskelbtiną informaciją ir kuriais leidžiama pasiekti naudotojo ar įrenginio duomenis dėl neatskleistų, neįdiegtų ar neleistinių funkcijų arba tokiais tikslais. Asmens ar neskelbtini duomenys, pasiekiami per leidimus ar API, kurie pasiekia neskelbtiną informaciją, niekada negali būti parduodami ar bendrinami, siekiant palengvinti pardavimą.

Leidimų pasiekti duomenis ir API, kurie gali pasiekti neskelbtiną informaciją, užklauskas teikite pagal kontekstą (pateikdami užklauskas keliais veiksmais), kad naudotojai suprastų, kodėl programa prašo leidimo. Duomenis naudokite tik tais tikslais, dėl kurių naudotojas sutiko. Jei vėliau duomenis norėsite naudoti kitais tikslais, turėsite to paprašyti naudotojų ir įsitikinti, kad jie sutinka su papildomais naudojimo būdais.

Riboti leidimai

Be anksčiau nurodytų apribojimų, riboti leidimai – tai leidimai, kurie nurodyti kaip [pavojingi](#) , [specialūs](#) ar [reikalaujantys parašo](#) , kaip nurodyta toliau. Šiems leidimams taikomi toliau nurodyti papildomi reikalavimai ir apribojimai.

- Naudotojo ar įrenginio duomenys, kuriuos pasiekti galima tik suteikus ribotus leidimus, laikomi asmens ir neskelbtiniais naudotojo duomenimis. Taikomi [naudotojų duomenų politikos](#) reikalavimai.
- Atsižvelkite į naudotojų sprendimą, jei jie atmeta riboto leidimo užklausą. Negalima manipuliuoti naudotojais ar jų versti sutikti su jokių neesminių leidimų. Turite stengtis prisiderinti prie naudotojų, kurie nesuteikia prieigos prie neskelbtinų duomenų (pvz., jei naudotojai yra apriboję prieigą prie skambučių žurnalų, leisti jiems patiems įvesti telefono numerį).
- Naudoti leidimus pažeidžiant „Google Play“ [kenkėjiškų programų politiką](#) (įskaitant [piktnaudžiavimo aukštesnio lygio privilegijomis politiką](#)) griežtai draudžiama.

Tam tikriems ribotiems leidimams gali būti taikomi papildomi toliau nurodyti reikalavimai. Šių apribojimų tikslas yra apsaugoti naudotojų privatumą. Labai retais atvejais galime taikyti ribotų toliau nurodytų reikalavimų išimčių, kai programoje teikiama labai svarbi ar esminė funkcija ir nėra alternatyvaus metodo funkcijai teikti. Įvertiname siūlomas išimtis atsižvelgdami į galimą poveikį naudotojų privatumui ar saugai.

SMS ir skambučių žurnalų leidimai

SMS ir skambučių žurnalų leidimai laikomi asmens ir neskelbtiniais naudotojo duomenimis, vadovaujantis [asmens ir neskelbtinos informacijos](#) politika bei toliau pateiktais apribojimais.

Ribotas leidimas	Reikalavimas
Skambučių žurnalo leidimų grupė (pvz., READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Įrenginyje ji turi būti aktyviai užregistruota kaip numatytoji telefono arba pagalbinė doroklė.
SMS leidimų grupė (pvz., READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Įrenginyje ji turi būti aktyviai užregistruota kaip numatytoji SMS arba pagalbinė doroklė.

Programos, kuriose nėra galimybės nustatyti numatytųjų SMS, Telefono ar Padėjėjo doroklės, gali neleisti apraše naudoti pirmiau nurodytų leidimų. Tai apima rezervuotos vietos tekstą apraše. Taip pat prieš raginant naudotojus sutikti su bet kuriuo iš pirmiau nurodytų leidimų, programos turi būti aktyviai užregistruotos kaip numatytosios SMS, Telefono ar Padėjėjo doroklės. Programa turi nedelsdama nustoti naudoti leidimą, kai nebėra numatytoji doroklė. Leidžiami naudojimo metodai ir išimty pasiekiami [šiose pagalbos centro puslapyje](#).

Programos leidimą (ir bet kokius su juo susijusius duomenis) gali naudoti tik patvirtintoms svarbiausioms programos funkcijoms teikti. Pagrindinės funkcijos apibrėžiamos kaip pagrindinė programos paskirtis. Tai gali apimti pagrindinių funkcijų, kurios turi būti aiškiai dokumentuojamos ir akcentuojamos programos apraše, rinkinį. Be pagrindinės (-ių) funkcijos (-ių) programa yra sugadinta arba pateikiama kaip nenaudojama. Šiuos duomenis perduoti, bendrinti ar naudoti pagal licenciją galima tik siekiant programoje teikti pagrindines funkcijas ar paslaugas, ir šių duomenų naudojimo negalima išplėsti jokių kitu tikslu (pvz., kitų programų ar paslaugų tobulinimo, reklamavimo ar rinkodaros tikslais). Negalite naudoti kitų metodų (įskaitant kitus leidimus, API ar trečiosios šalies šaltinius) siekdami gauti duomenis, priskirtus su skambučių žurnalu ar SMS susijusiems leidimams.

Leidimas pasiekti vietovės duomenis

[Įrenginio vietovė](#) laikoma asmens ir neskelbtiniais naudotojo duomenimis, kuriems taikoma [asmens ir neskelbtinos informacijos](#) politika, [fone veikiančios vietovės nustatymo funkcijos politika](#) ir toliau pateikti reikalavimai.

- Programos negali pasiekti duomenų, saugomų pagal leidimus pasiekti vietovės duomenis (pvz., ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION), jei jie nebereikalingi norint teikti dabartines funkcijas ar paslaugas programoje.
- Niekada neprašykite naudotojų leidimų pasiekti vietovės duomenis, jei jų reikia tik reklamai ar analizei. Programos, praplečiančios leidžiamą šių duomenų naudojimą siekiant teikti skelbimus, turi atitikti [skelbimų politiką](#).
- Programose turi būti prašoma mažiausios apimtys prieigos (pvz., apytikslės vietoje tikslios ir priekinio plano vietoje fono), reikalingos vietovės reikalaujančiai dabartinei funkcijai ar paslaugai teikti, ir naudotojai turėtų numatyti, kad funkcijai ar paslaugai reikalinga prašomo vietovės lygio informacija. Pvz., galime at mesti programas, prašančias foninės vietovės ar ją pasiekiančias be tinkamo pagrindo.
- Fone veikiančią vietovės nustatymo funkciją galima naudoti tik naudotojams naudingoms funkcijoms, susijusioms su pagrindinėmis programos funkcijomis, teikti.

Programoms leidžiama pasiekti vietovę naudojant priekinio plano paslaugas (kai programa turi tik prieigą priekiniame plane, pvz., „kol naudojama“) leidimą, jei naudoti:

- pradėta tęsiant programos naudotojo pradėtą veiksmą ir
- baigiama iškart, kai programa užbaigia numatyto naudotojo pradėto veiksmo atvejį.

Būtent vaikams skirtos programos turi atitikti politiką [„Skirta šeimai“](#).

Jei reikia daugiau informacijos apie politikos reikalavimus, žr. šį [pagalbos centro straipsnį](#).

Visų failų prieigos leidimas

Naudotojo įrenginyje esantys failai ir katalogo atributai laikomi asmens ir neskelbtiniais naudotojo duomenimis, vadovaujantis [asmens ir neskelbtinos informacijos](#) politika bei toliau pateiktais reikalavimais.

- Programos turėtų pateikti užklausą pasiekti tik įrenginio saugyklą, kuri yra būtina, kad programa veiktų, ir negali teikti užklausų dėl prieigos prie įrenginio saugyklos trečiosios šalies vardu jokiais tikslais, nesusijusiais su svarbiausiomis naudotojams skirtomis programos funkcijomis.
- „Android“ įrenginiams, kuriuose veikia R arba naujesnė versija, reikės leidimo [MANAGE_EXTERNAL_STORAGE](#), kad būtų galima tvarkyti prieigą prie bendrinamos saugyklos. Visos programos, kurios taikomos pagal R versiją ir prašo suteikti plačią prieigą prie bendrinamos saugyklos („Visų failų prieiga“), prieš jas paskelbiant turi atitikti atitinkamos prieigos peržiūros reikalavimus. Programos, kurioms leidžiama naudoti šį leidimą, turi aiškiai paraginti naudotojus įgalinti „Visų failų prieigą“ programos nustatymuose „Speciali prieiga prie programų“. Jei reikia daugiau informacijos apie R reikalavimus, žr. šį [pagalbos straipsnį](#).

Paketo (programos) matomumo leidimas

Įdiegtos programos, kurių užklausos teiktos iš įrenginio, laikomos asmens ir neskelbtiniais naudotojo duomenimis pagal [asmens ir neskelbtinos informacijos](#) politiką bei toliau nurodytus reikalavimus.

Programoms, kurių pagrindinis tikslas yra paleisti kitas įrenginio programas, jų ieškoti ar su jomis sąveikauti, gali būti suteikiamas pagal taikymo sritį tinkamas kitų įrenginyje įdiegtų programų matomumo lygis, kaip nurodyta toliau.

- **Platus programos matomumas:** platus matomumas yra programos galimybė išplėstai (arba plačiai) matyti įrenginyje įdiegtas programas (paketus).
 - Programoms, taikomoms pagal [30 ar aukštesnio lygio API](#), platus įdiegtų programų matomumas naudojant leidimą [QUERY_ALL_PACKAGES](#) suteikiamas tik konkrečiais naudojimo atvejais, kai programa turi aptikti ir (arba) sąveikauti su kuria nors ar visomis įrenginyje esančiomis programomis, kad galėtų veikti.
 - Negalite naudoti leidimo [QUERY_ALL_PACKAGES](#), jei programa gali veikti naudojant geriau [pritaikytos taikymo srities paketo matomumo deklaraciją](#) (pvz., teikdama užklausas ir sąveikaudama su konkrečiais paketais, o ne teikdama plataus matomumo užklausas).
 - Naudoti alternatyvius metodus siekiant apytiksliai įvertinti plataus matomumo lygį, susijusį su leidimu [QUERY_ALL_PACKAGES](#), taip pat leidžiama tik naudotojams teikiamoms pagrindinėms programos funkcijoms ir sąveikai su bet kokiais programomis, aptiktomis naudojant šį metodą.
 - Leidžiamas leidimo [QUERY_ALL_PACKAGES](#) naudojimo atvejus galite peržiūrėti šiame [pagalbos centro straipsnyje](#).
- **Apribotas programos matomumas:** apribotas matomumas – tai toks matomumas, kai programa sumažina galimybę pasiekti duomenis teikdama konkrečių programų užklausas geriau pritaikytais (o ne plačiais) metodais (pvz., teikdama konkrečių programų, atitinkančių programos aprašo deklaraciją, užklausas). Naudodami šį metodą galite teikti programų užklausas tokiais atvejais, kai programa yra suderinama pagal politiką arba valdo šias programas.
- Įrenginyje įdiegtų programų skelbimų vietų matomumas turi būti tiesiogiai susijęs su pagrindiniu programos tikslu ar pagrindinėmis funkcijomis, kurias naudotojai pasiekia programoje.

Programos skelbimų vietų duomenų, gaunamų iš „Play“ platinamų programų, negalima parduoti ar bendrinti analizės ar pajamų gavimo tikslais.

Pritaikomumo API

Pritaikomumo API negalima naudoti siekiant:

- pakeisti naudotojo nustatymus be jo leidimo ar neleisti naudotojams išjungti ar pašalinti bet kokios programos ar paslaugos, išskyrus atvejus, kai tai daryti įgaliojo vienas iš tėvų ar globėjų,

naudodamas tėvų kontrolės programą, arba įgaliojimą suteikė administratoriai per įmonės tvarkymo programinę įrangą;

- apeiti „Android“ įtaisytuosius privatumo valdiklius ir pranešimus arba
- naudotojo sąsają pakeisti ar paveikti tokiu būdu, kuris yra apgaulingas ar kitaip pažeidžia „Google Play“ kūrėjų politiką.

Pritaikomumo API nėra skirta nuotoliniams skambučių garso įrašams ir negali būti teikiama tokia jos užklausa.

Pritaikomumo API naudojimas turi būti nurodytas „Google Play“ įrašė.

IsAccessibilityTool gairės

Programos, kurių pagrindinė funkcija yra tiesioginė pagalba neįgaliesiems, gali naudoti **IsAccessibilityTool**, kad viešai būtų nurodomos kaip pritaikomumo programos.

Programos, kurios negali naudoti **IsAccessibilityTool**, neprivalo naudoti žymos ir privalo atitikti aiškaus paskelbimo bei sutikimo reikalavimus, nurodytus [naudotojo duomenų politikoje](#), nes su pritaikomumu susijusios funkcijos nėra aiškos naudotojui. Jei reikia daugiau informacijos, žr. pagalbos centro straipsnį apie [„AccessibilityService“ API](#).

Kai įmanoma, vietoj pritaikomumo API programose turi būti naudojami siauresnės apimties [API ir leidimai](#), užtikrinantys pageidaujamų funkcijų veikimą.

Diegimo paketų užklauso leidimas

Suteikus leidimą [REQUEST_INSTALL_PACKAGES](#) programai leidžiama teikti programos paketų diegimo užklausa. Norint naudoti šį leidimą, jūsų programos pagrindinės funkcijos turi apimti:

- programos paketų siuntimą arba gavimą ir
- naudotojo inicijuoto programos paketų diegimo įgalinimą.

Leidžiamos funkcijos

- Žiniatinklio naršymas ar paieška
- Priedus palaikančios ryšio paslaugos
- Failų bendrinimas, perkėlimas arba valdymas
- Įmonių įrenginių tvarkymas
- Atsarginė kopija ir atkūrimas
- Įrenginio perkėlimas ir (arba) telefono perkėlimas
- Papildoma programa, skirta telefonui sinchronizuoti su nešiojamuoju ar ISĮ įrenginiu (pvz., išmaniuoju laikrodžiu ar išmaniuoju televizoriumi)

Pagrindinės funkcijos apibrėžiamos kaip pagrindinė programos paskirtis. Pagrindinė funkcija ir visos ją sudarančios pagrindinės funkcijos turi būti aiškiai dokumentuojamos ir akcentuojamos programos apraše.

Leidimo [REQUEST_INSTALL_PACKAGES](#) negalima naudoti savarankiškiems atnaujinimams, keitimams ar kitų APK grupavimo veiksams išteklių faile, nebent siekiama tvarkyti įrenginį. Visi naujiniai ar paketų diegimai turi atitikti „Google Play“ [piktnaudžiavimo įrenginiu ir tinklu politiką](#) ir turi būti inicijuoti bei vykdomi naudotojo.

„Android“ teikiamos sistemoje „Health Connect“ leidimai

[„Health Connect“](#) – tai „Android“ platforma, kurioje sveikatos ir kūno rengybos programos gali saugoti ir bendrinti tuos pačius įrenginyje esančius duomenis vienoje ekosistemoje. Be to, naudotojai gali vienoje vietoje valdyti, kurios programos gali skaityti ir rašyti sveikatos ir kūno rengybos duomenis. „Health Connect“ palaiko [įvairių tipų duomenų](#), įskaitant žingsnių skaičių ir kūno temperatūrą, skaitymą ir rašymą.

Duomenys, pasiekiami naudojant „Health Connect“ leidimus, laikomi naudotojo asmens ir neskelbtiniais duomenimis, vadovaujantis [naudotojų duomenų politika](#). Jei jūsų programa atitinka sveikatos programos reikalavimus arba joje teikiamos su sveikata susijusios funkcijos ir ji pasiekia sveikatos duomenis, įskaitant „Health Connect“ duomenis, ji taip pat turi atitikti [sveikatos programų politikos reikalavimus](#).

Žr. šį [„Android“ kūrėjų vadovą](#), kaip pradėti naudoti „Health Connect“. Jei norite pateikti užklausą dėl prieigos prie „Health Connect“ duomenų tipų, žr. [čia](#).

Sistemoje „Google Play“ platinamos programos turi atitikti toliau nurodytus politikos reikalavimus, kad galėtų skaityti ir (arba) rašyti duomenis sistemoje „Health Connect“.

Tinkama prieiga prie sistemos „Health Connect“ ir jos naudojimas

„Health Connect“ galima naudoti tik laikantis galiojančios politikos, taisyklių ir nuostatų bei atsižvelgiant į patvirtintus naudojimo atvejus, išdėstytus šioje politikoje. Tai reiškia, kad prieigos prie leidimų užklausą galite teikti, tik kai programa ar paslauga atitinka vieną iš patvirtintų naudojimo atvejų.

Patvirtinti naudojimo atvejai apima kūno rengybos ir sveikatinimo, premijų, kūno rengybos trenerių, įmonių sveikatinimo, medicininės priežiūros, sveikatos tyrimų ir žaidimų programas. Programose, kurioms suteikta prieiga prie šių leidimų, negalima išplėsti naudojimo neatskleistais ar neleistiniais tikslais.

Tik programoms ar paslaugoms, kuriose yra bent viena funkcija, kurios pagrindinis tikslas padėti naudotojams rūpintis sveikata ir kūno rengyba, leidžiama teikti prieigos prie „Health Connect“ leidimų užklausą. Tai apima toliau nurodytas programas ar paslaugas.

- Programos arba paslaugos, leidžiančios naudotojams **tiesiogiai įrašyti, pranešti, stebėti ir (arba) analizuoti** savo fizinę veiklą, miego būseną, psichikos sveikatą, mitybą, sveikatos būklės įvertinimus, fizinius aprašus ir (arba) kitus su sveikata ar kūno rengyba susijusius aprašus ir įvertinimus.
- Programos arba paslaugos, leidžiančios naudotojams **saugoti savo fizinės veiklos, miego būsenos, psichikos sveikatos, mitybos duomenis, sveikatos būklės įvertinimus, fizinius aprašus** ir (arba) kitus su sveikata ar kūno rengyba susijusius aprašus ir įvertinimus telefone ir (arba) nešiojamajame įrenginyje bei bendrinti duomenis su kitomis šių naudojimo atvejų reikalavimus atitinkančiomis programomis įrenginyje.

Prieigos prie „Health Connect“ negalima naudoti pažeidžiant šią politiką ar kitas galiojančias „Health Connect“ taisykles ir nuostatas ar politiką, įskaitant naudojimą toliau nurodytais tikslais.

- Nenaudokite „Health Connect“ kurdami ar įtraukdami į programas, aplinką ar veiklą, kai naudojant „Health Connect“ ar įvykus sistemos trikdžiai pagrįstai gali kilti mirties, asmens sužalojimo ar žalos aplinkai arba turtui pavojus (pvz., kuriant ar valdant branduolinius įrenginius, eismo ore kontrolę, gyvybės palaikymo sistemas ar ginkluotę).
- Nenaudokite duomenų, gautų per „Health Connect“, naudodami programas be grafinės naudotojo sąsajos. Programa turi turėti aiškiai atpažįstamą piktogramą programų dėkle, įrenginio programos nustatymus, pranešimų piktogramas ir t. t.
- Nenaudokite „Health Connect“ su programomis, sinchronizuojančiomis duomenis su nesuderinamais įrenginiais ar platformomis.
- Nenaudokite „Health Connect“ norėdami prisijungti prie programų, paslaugų ar funkcijų, kurios skirtos tik vaikams.
- Imkitės protingų ir tinkamų veiksmų, kad apsaugotumėte visas programas ar sistemas, naudojančias „Health Connect“, nuo neįgalios ar neteisėtos prieigos, naudojimo, panaikinimo, praradimo, keitimo ar paskelbimo.

Be to, privalote užtikrinti, kad būtų laikomasi visų reguliavimo ar teisinių reikalavimų, kurie gali būti taikomi, atsižvelgiant į jūsų numatomą „Health Connect“ naudojimą ir bet kokius iš „Health Connect“ gaunamus duomenis. Jei nėra aiškiai nurodyta „Google“ pateiktame konkrečių „Google“ produktų ar paslaugų žymėjime ar informacijoje, „Google“ nepatvirtina jokių duomenų, esančių sistemoje „Health

Connect“, naudojimo ir negarantuoja jų tikslumo bet kokio naudojimo atveju ar bet koku tikslu, ypač tais atvejais, kai duomenys naudojami tyrimo, sveikatos ar mediciniais tikslais. „Google“ atsisako bet kokios atsakomybės, susijusios su duomenų, gautų per sistemą „Health Connect“, naudojimu.

Ribotas naudojimas

Naudojant „Health Connect“ taikomi tam tikri prieigos prie duomenų ir jų naudojimo apribojimai.

- Duomenys gali būti naudojami tik siekiant teikti ar tobulinti atitinkamą naudojimo atvejį ar funkcijas, matomus programos naudotojo sąsajoje.
- Naudotojo duomenis galima perkelti trečiosioms šalims tik gavus aiškų naudotojo sutikimą: siekiant užtikrinti saugą (pvz., nagrinėjant piktnaudžiavimą), laikantis galiojančių įstatymų ar reglamentų arba vykdamas sujungimus ar įsigijimus.
- Žmonių prieiga prie naudotojų duomenų ribojama, nebent gaunamas aiškus naudotojo sutikimas, siekiant užtikrinti saugą, laikantis galiojančių įstatymų ar renkant duomenis, kad būtų galima atlikti vidines operacijas, vadovaujantis teisiniais reikalavimais.
- Bet kokio kito tipo „Health Connect“ duomenų perkėlimas, naudojimas ar pardavimas draudžiamas, įskaitant:
 - naudotojo duomenų perkėlimą ar pardavimą trečiosioms šalims, pvz., reklamavimo platformoms, duomenų brokeriams ar bet kokiems informacijos perpardavėjams;
 - naudotojo duomenų perkėlimą, pardavimą ar naudojimą skelbimams teikti, įskaitant suasmenintą reklamavimą arba reklamavimą pagal pomėgius;
 - naudotojo duomenų perkėlimą, pardavimą ar naudojimą norint nustatyti kreditingumą ar skolinimo tikslais;
 - naudotojo duomenų perkėlimą, pardavimą ar naudojimą su bet koku produktu ar paslauga, kurie gali būti laikomi medicininio įrenginio, vadovaujantis Federalinio maisto, vaistų ir kosmetikos įstatymo 201 skilties h skirsniu, jei naudotojo duomenys mediciniame įrenginyje bus naudojami jo reguliuojamai funkcijai vykdyti;
 - naudotojo duomenų perkėlimą, pardavimą ar naudojimą bet koku tikslu ar bet kokiomis priemonėmis, susijusiomis su Apsaugota sveikatos informacija (kaip apibrėžta HIPAA), nebent gaunate „Google“ išankstinį, rašytinį tokio naudojimo patvirtinimą.

Minimali aprėptis

Turite teikti tik prieigos prie leidimų, kurie yra būtini, kad galėtumėte diegti produkto funkcijas ar paslaugas, užklaudas. Tokios prieigos užklaudos turi būti konkrečios ir apimti tik reikalingus duomenis.

Skaidrus ir tikslus pranešimas bei valdymas

„Health Connect“ tvarko sveikatos ir kūno rengybos duomenis, įskaitant neskelbtiną informaciją, ir reikalauja, kad visose programose būtų taikoma išsami privatumo politika. Privatumo politikoje turi būti aiškiai nurodyta, kaip programoje renkami, naudojami ir bendrinami naudotojų duomenys. Be teisinių reikalavimų, kūrėjai turi pateikti toliau nurodytą informaciją privatumo politikoje.

- Tikslus programos aprašas, nurodant pasiekiamus duomenis ir jų ryšį su reikšmingomis programos funkcijomis ar rekomendacijomis
- Duomenų saugojimo ir ištrynimo praktika
- Duomenų apdorojimo procedūros. Pvz., jų perdavimas naudojant modernią kriptografiją (pvz., naudojant HTTPS).

Saugus duomenų apdorojimas

Visi naudotojo duomenys turi būti saugiai apdorojami. Imkitės protingų ir tinkamų veiksmų, kad apsaugotumėte visas programas ar sistemas, naudojančias „Health Connect“, nuo neįgalios ar neteisėtos prieigos, naudojimo, panaikinimo, praradimo, keitimo ar paskelbimo.

Rekomenduojama saugos praktika apima Informacijos saugos valdymo sistemos diegimą, kaip apibrėžta ISO/IEC 27001, ir užtikrinimą, kad programa arba žiniatinklio paslauga yra patikima bei joje nėra dažnai pasitaikančių saugos problemų, nurodytų OWASP dešimt dažniausiai pasitaikančių problemų sąrašė.

Atsižvelgdami į pasiekiamą API ir naudotojų leidimų ar naudotojų skaičių, reikalausime, kad būtų atliktas programos ar paslaugos periodinis saugos įvertinimas ir gautas įvertinimo laiškas iš [paskirtos trečiosios šalies](#), jei naudojant jūsų produktą perkeliama duomenys iš naudotojo įrenginio.

Jei reikia daugiau informacijos apie programoms, prisijungiančioms prie „Health Connect“, taikomus reikalavimus, žr. šį [pagalbos straipsnį](#).

VPN paslauga

„VpnService“ yra pagrindinė programų klasė, kur galima išplėsti ir kurti savo VPN priemones. Tik programose, kuriose naudojama „VpnService“ ir nustatytas VPN kaip pagrindinės funkcijos, galima kurti saugų įrenginio lygio tunelinį ryšį su nuotoliniu serveriu. Išimtys taikomos programoms, kurioms reikalingas nuotolinis serveris pagrindinėms funkcijoms vykdyti. Toliau pateikiama pavyzdžių.

- Tėvų kontrolės ir įmonių valdymo programos.
- Programų naudojimo stebėjimas.
- Įrenginių saugos užtikrinimo programos (pvz., antivirusinės, mobiliųjų įrenginių valdymo, užkardos programos).
- Su tinklu susiję įrankiai (pvz., nuotolinė prieiga).
- Žiniatinklio naršymo programos.
- Operatorių programos, kurias naudojant reikalingos VPN funkcijos, kad būtų galima teikti telefonijos ar ryšio paslaugas.

„VpnService“ negalima naudoti norint atlikti toliau nurodytus veiksmus.

- Rinkti asmens ir neskelbtinus naudotojų duomenis be aiškaus paskelbimo ir sutikimo.
- Peradresuoti naudotojų srautą iš kitų programų įrenginyje ar juo manipuluoti siekiant gauti pajamų (pvz. peradresuoti skelbimų srautą per kitą nei naudotojo šalį).

Programose, kuriose naudojama „VpnService“, būtina laikytis toliau nurodytų reikalavimų.

- Būtina dokumentuoti „VpnService“ naudojimą „Google Play“ įrašė.
- Būtina šifruoti duomenis, perduodamus iš įrenginio į VPN tunelinio ryšio galutinį tašką.
- Būtina laikytis visų [Kūrėjų programos politikos](#) nuostatų, įskaitant [apgaulingų skelbimų](#), [leidimų](#) ir [kenkėjiškų programų](#) politikos nuostatas.

Tikslaus signalo leidimas

Programose, teikiamose ne senesnės nei tryliktos versijos sistemoje „Android“ (33 tikslinio API lygio), bus pristatytas naujas leidimas `USE_EXACT_ALARM`, kuriuo bus leidžiama pasiekti [tikslaus signalo funkcijas](#).

`USE_EXACT_ALARM` yra ribotas leidimas, kuris programose turi būti apibrėžtas, tik jei tikslus signalas reikalingas jų pagrindinėms funkcijoms vykdyti. Programos, kuriose pateikiama šio riboto leidimo užklausa, peržiūrimos. Programų, kurios neatitinka priimtino naudojimo atvejų kriterijų, neleidžiama skelbti sistemoje „Google Play“.

Priimtino tikslaus signalo leidimo naudojimo atvejai

`USE_EXACT_ALARM` funkcijos gali būti naudojamos programoje, tik kai programos pagrindinėms, naudotojams teikiamoms funkcijoms vykdyti reikalingi tikslaus laiko veiksmai, pvz.:

- programa yra žadintuvo arba laikmačio programa;
- programa yra kalendoriaus programa, kurioje rodomi įvykių pranešimai.

Jei jūsų tikslaus signalo funkcijų naudojimo atvejis nenurodytas anksčiau, turite įvertinti, ar galite naudoti alternatyvų leidimą `SCHEDULE_EXACT_ALARM`.

Jei reikia daugiau informacijos apie tikslaus signalo funkcijas, žr. šias [kūrėjams skirtas gaires](#).

Viso ekrano tikslo leidimas

Programose, kurios taikomos pagal 14 ar naujesnės versijos „Android“ (34 tikslinio lygio API), `USE_FULL_SCREEN_INTENT` yra [specialios programų prieigos leidimas](#). Programoms bus automatiškai suteiktas `USE_FULL_SCREEN_INTENT` leidimas, tik jei programos pagrindinės funkcijos patenka į vieną iš toliau nurodytų kategorijų, kurioms reikalingi didelio prioriteto pranešimai.

- Signalo nustatymas
- Telefonų ar vaizdo skambučių gavimas

Programos, kuriose pateikiama šio leidimo užklausa, peržiūrimos. Programoms, kurios neatitinka anksčiau nurodytų kriterijų, nebus automatiškai suteiktas šis leidimas. Tokiu atveju programose turi būti naudotojui pateikta leidimo naudoti `USE_FULL_SCREEN_INTENT` užklausa.

Primename, kad naudojant `USE_FULL_SCREEN_INTENT` leidimą visada būtina laikytis visų „Google Play“ politikos programų kūrėjams nuostatų, įskaitant [mobiliesiems skirtos nepageidaujamos programinės įrangos](#), [piktnaudžiavimo įrenginiu ir tinklu](#) ir [skelbimų](#) politikos nuostatas. Teikiant viso ekrano režimo pranešimus negalima neteisėtai trikdyti, pažeisti ar pasiekti naudotojo įrenginį. Be to, programos neturėtų trukdyti kitoms programoms ar naudoti įrenginį.

Sužinokite daugiau apie leidimą `USE_FULL_SCREEN_INTENT` mūsų [pagalbos centre](#).

Piktnaudžiavimas įrenginiu ir tinklu

Neleidžiame teikti programų, kurios neteisėtai trikdo, pažeidžia ar pasiekia naudotojo įrenginį, kitus įrenginius ar kompiuterius, serverius, tinklus, programų programavimo sąsajas (API) ar paslaugas, įskaitant (bet tuo neapsiribojant) kitas įrenginyje esančias programas, bet kokią „Google“ paslaugą ar įgaliojotojo teikėjų tinklą.

Sistemoje „Google Play“ teikiamos programos turi atitikti numatytuosius „Android“ sistemos optimizavimo reikalavimus, nurodytus [pagrindinėse „Google Play“ programų kokybės gairėse](#).

Sistemoje „Google Play“ platinama programa negali pati modifikuotis, pasikeisti ar atsinaujinti naudodama kitą metodą nei „Google Play“ atnaujinimo mechanizmą. Be to, programa negali atsisiųsti vykdomojo kodo (pvz., „dex“, JAR ar .so failų) iš kito šaltinio nei „Google Play“. Šis apribojimas netaikomas kodui, kuris vykdomas virtualiajame kompiuteryje arba interpretatorijoje, suteikiančiame netiesioginę prieigą prie „Android“ API (pvz., „JavaScript“ žiniatinklio rodinyje arba naršyklėje).

Programos ar trečiosios šalies kodas (pvz., SDK) su interpretuojamomis kalbomis („JavaScript“, „Python“, „Lua“ ir pan.), įkeliami paleidžiant (pvz., neįtraukti į programos paketą), negali kelti „Google Play“ politikos nuostatų pažeidimo rizikos.

Neleidžiame naudoti kodo, kuriame yra saugos pažeidimų. Peržiūrėkite [programų saugumo tobulinimo paslaugą](#) ir sužinokite apie naujausias saugos problemas, apie kurias pranešta kūrėjams.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

Dažnai pasitaikančių piktnaudžiavimo įrenginiu ir tinklu pažeidimų pavyzdžiai.

- Programos, kurios blokuoja ar trikdo kitas skelbimus teikiančias programas.
- Sukčiavimo žaidžiant žaidimus programos, paveikiančios kitų programų žaidimo eigą.
- Programos, kurios padeda ar teikia instrukcijas, kaip užgrobti paslaugas, programinę įrangą ar aparatinę įrangą arba apeiti saugos priemones.
- Programos, kurios pasiekia ar naudoja paslaugą arba API pažeisdamos paslaugų teikimo sąlygas.

- Programos, kurių [negalima įtraukti į leidžiamųjų sąrašą](#) ir kurios bando apeiti [sistemos maitinimo valdymą](#).
- Programos, trečiosioms šalims palengvinančios naudojimąsi tarpinio serverio paslaugomis, gali tai daryti tik tokiu atveju, jei tai yra pagrindinė ir svarbiausia naudotojui teikiama programos funkcija.
- Programos ar trečiosios šalies kodas (pvz., SDK), atsisiuoiantys vykdomąjį kodą, pvz., „dex“ failus arba savąjį kodą, iš kito šaltinio nei „Google Play“.
- Programos, kurios įrenginyje įdiegia kitas programas be išankstinio naudotojo sutikimo.
- Programos, kurios padeda platinti ar įdiegti kenkėjišką programinę įrangą arba nukreipia į tam skirtas vietas.
- Programos ar trečiosios šalies kodas (pvz., SDK), apimantys žiniatinklio rodinį su pridėta „JavaScript“ sąsaja, įkeliančia nepatikimą žiniatinklio turinį (pvz., http:// URL) arba nepatvirtintus URL, gautus iš nepatikimų šaltinių (pvz., URL, gautus su nepatikimais tikslais).
- Programos, kuriose naudojamas [viso ekrano režimo tikslo leidimas](#), siekiant priversti naudotoją sąveikauti su veikimą trikdančiais skelbimais ar pranešimais.

Priekinio plano paslaugos naudojimas

Priekinio plano paslaugų leidimas užtikrina tinkamą naudotojui matomų priekinio plano paslaugų naudojimą. Programoms, kurios skirtos 14 ar naujesnės versijos „Android“, turite nurodyti galiojantį kiekvienos programoje naudojamos priekinio plano paslaugos tipą ir apibrėžti šiam tipui tinkamą [priekinio plano paslaugų leidimą](#). Pavyzdžiui, jei naudojant jūsų programą reikia žemėlapių geografinės vietovės nustatymo, turite apibrėžti [FOREGROUND_SERVICE_LOCATION](#) leidimą programos apraše.

Programoms leidžiama apibrėžti priekinio plano paslaugos leidimą, jei naudojant:

- teikiama naudotojams naudinga funkcija, susijusi su pagrindinėmis programos funkcijomis;
- funkcijos inicijuojamos naudotojo arba pastebimos naudotojui (pavyzdžiui, garsas iš leidžiamos dainos, į kitą įrenginį perduodama medija, tikslus ir aiškus pranešimas naudotojui, naudotojo užklausa įkelti nuotrauką į debesį);
- naudotojas gali jas nutraukti ar sustabdyti;
- sistema negali jų nutraukti ar atidėti, nesukeldama neigiamos naudotojo patirties arba neleisdama naudotojui numatytai funkcijai veikti taip, kaip numatyta (pvz., telefono skambutis turi būti pradėtas nedelsiant ir sistema negali jo atidėti);
- jos leidžiamos tik tiek, kiek reikia užduočiai pabaigti.

Toliau nurodytiems priekinio plano paslaugos naudojimo atvejams taikoma anksčiau pateiktų kriterijų išimtis.

- Priekinio plano paslaugų tipai [systemExempted](#) arba [shortService](#).
- Priekinio plano paslaugų tipas „dataSync“, tik naudojant „Play Asset Delivery“ funkcijas.

Priekinio plano paslaugos naudojimas išsamiau paaiškinamas [čia](#).

Naudotojo inicijuoto duomenų perdavimo darbai

Programoms leidžiama naudoti [naudotojo inicijuotų duomenų perkėlimo darbų](#) API tik kai:

- jos naudojamos inicijavus naudotojui;
- naudojamos tinklo duomenų perkėlimo užduotims;
- leidžiamos tik tiek, kiek reikia duomenų perkėlimui pabaigti.

Naudotojo inicijuotų duomenų perkėlimo API naudojimas išsamiau paaiškinamas [čia](#).

Saugą užtikrinančios žymos reikalavimai

[FLAG_SECURE](#) – tai programos kode apibrėžta rodoma žyma, nurodanti, kad šioje NS yra neskelbtinų duomenų, kurie gali būti rodomi tik saugioje platformoje, naudojant programą. Ši žyma skirta neleisti rodyti duomenų ekrano kopijose ar peržiūrėti jų nesaugiuose ekranuose. Kūrėjai

apibrėžia šią žymą, kai programos turinio negalima transliuoti, peržiūrėti ar kitaip perduoti iš programos ar naudotojų įrenginių.

Siekiant užtikrinti saugą ir privatumą, visose sistemoje „Google Play“ platinamose programose būtina atsižvelgti į kitų programų FLAG_SECURE apibrėžtį. Tai reiškia, kad programose negali būti palaikomos ar kuriamos priemonės FLAG_SECURE nustatymams kitose programose apeiti.

Programoms, kurios priskiriamos [pritaikomumo įrankio](#) kategorijai, šis reikalavimas netaikomas, jei jose neperduodamas, neišsaugomas ar nesaugomas talpykloje FLAG_SECURE apsaugotas turinys, kad jį būtų galima pasiekti ne naudotojo įrenginyje.

Programos, kurios paleidžia „Android“ sudėtinius failus įrenginyje

„Android“ sudėtinių failų įrenginyje programos teikia aplinką, imituojančią visą pagrindinę „Android“ OS arba jos dalis. Šios aplinkos funkcijos gali atspindėti ne visą „Android“ saugos funkcijų komplektą, todėl kūrėjai gali pasirinkti pridėti saugios aplinkos aprašo žymą, kad nurodytų „Android“ sudėtiniams failams įrenginyje, jog jie neturėtų būti vykdomi jų imituojamoje „Android“ aplinkoje.

Saugios aplinkos aprašo žyma

[REQUIRE_SECURE_ENV](#) – tai žyma, kurią galima apibrėžti programos apraše, norint nurodyti, kad šios programos negalima vykdyti „Android“ sudėtinių failų programose įrenginyje. Siekiant užtikrinti saugą ir privatumą, programose, kuriose teikiami „Android“ sudėtiniai failai įrenginyje, būtina atsižvelgti į visas programas, kuriose apibrėžta ši žyma, ir:

- Peržiūrėkite programų aprašus, kuriuos jos ketina įkelti „Android“ sudėtiniame faile įrenginyje pagal šią žymą.
- Neįkelkite programų, kurių „Android“ sudėtiniame faile įrenginyje apibrėžta ši žyma.
- Neveikite kaip tarpinis serveris, perimdami ar iškviesdami API įrenginyje, lyg jie būtų įdiegti sudėtiniame faile.
- Neskaitinkite kurti ir nekurkite priemonių, kuriomis būtų galima apeiti žymą (pvz., įkeliant senesnės versijos programą, siekiant apeiti dabartinės programos žymą REQUIRE_SECURE_ENV).

Sužinokite daugiau apie šią politiką [pagalbos centre](#).

Apgaulinga elgsena

Neleidžiame teikti programų, kuriose bandoma apgauti naudotojus ar įgalinti nesąžiningą elgesį, įskaitant programas (bet jomis neapsiribojant), kurių funkcijos negali būti vykdomos. Programose turi būti pateiktas tikslus jos funkcijų paskelbimo pranešimas, aprašas ir vaizdai / vaizdo įrašai visose metaduomenų dalyse. Programose negali būti kopijuojamos funkcijos ar įspėjimai iš operacinės sistemos ar kitų programų. Bet kokie įrenginio nustatymų pakeitimai turi būti atliekami pranešus naudotojui ir gavus jo sutikimą ir jie turi būti grąžinami.

Klaidinantys teiginiai

Neleidžiame teikti programų, kurių apraše, pavadinime, piktogramoje ar ekrano kopijose yra melagingos ar klaidinančios informacijos.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Programos, kurių funkcijos aprašytos klaidingai arba netiksliai.
 - Programa, kurios apraše ir ekrano kopijose nurodoma, kad tai lenktynių žaidimas, bet iš tikrųjų ji yra dëlionės žaidimas, kuriame naudojama automobilio nuotrauka.
 - Programa, kurioje nurodoma, kad tai antivirusinė programa, bet joje yra tik teksto vadovas, kuriame aiškinama, kaip pašalinti virusus.
- Programos, kuriose nurodomos negalimos įdiegti funkcijos, pvz., vabzdžius atbaidančios programos, net jei jos pateikiamos kaip išdaiga, klastotė, pokštas ir pan.

- Programos, kurios priskirtos netinkamai kategorijai, įskaitant (bet tuo neapsiribojant) programos įvertinimą ar programos kategoriją.
- Akivaizdžiai klaidinantis ar klaidingas turinys, galintis trikdyti balsavimo procesą, arba toks turinys apie rinkimų rezultatus.
- Programos, kuriose klaidingai nurodoma, kad jos yra susijusios su valdžios institucija arba kad jos teikia su valdžios institucijomis susijusias paslaugas, nors toks įgaliojimas nesuteiktas.
- Programos, kurios melagingai nurodo, kad yra oficiali žinomo subjekto programa. Neturint reikiamų leidimų ar teisių neleidžiama naudoti pavadinimų, pvz., „Oficiali Justino Bieberio programa“.

1. Šioje programoje teikiami su medicina ar sveikata susiję teiginiai (vėžio gydymas), kurie yra klaidinantys.
2. Šiose programose nurodomos funkcijos, kurių negalima įdiegti (naudojant telefoną kaip alkotesterį).

Apgaulingi įrenginio nustatymų pakeitimai

Neleidžiame teikti programų, kurios atlieka su programa nesusijusius naudotojo įrenginio nustatymų ar funkcijų pakeitimus be naudotojo žinios ir sutikimo. Įrenginio nustatymai ir funkcijos apima sistemos ir naršyklės nustatymus, žymes, sparčiuosius klavišus, valdiklius ir programų pristatymą pagrindiniame ekrane.

Be to, neleidžiami toliau pateikti elementai.

- Programos, kurios keičia įrenginio nustatymus ar funkcijas su naudotojo sutikimu, bet tai daro taip, kad grąžinti pakeitimus nėra lengva.
- Programos ar skelbimai, kurie keičia įrenginio nustatymus ar funkcijas kaip trečiųjų šalių paslauga ar reklamavimo tikslais.
- Programos, kurios klaidina naudotojus, kad jie pašalintų arba išjungtų trečiųjų šalių programas ar pakeistų įrenginio nustatymus ar funkcijas.
- Programos, kuriose naudotojai raginami ar skatinami pašalinti ar išjungti trečiųjų šalių programas arba pakeisti įrenginio nustatymus ar funkcijas, jei tai nėra programos teikiamų saugos paslaugų dalis.

Nesąžiningo elgesio įgalinimas

Neleidžiame programų, kurios padeda naudotojams klaidinti kitus asmenis ar pasižymi kita apgaulinga veikla, įskaitant programas (bet jomis neapsiribojant), generuojančias (ar padedančias generuoti) asmens tapatybės korteles, socialinio draudimo numerius, pasus, diplomus, kredito korteles, banko sąskaitas ir vairuotojų pažymėjimus. Programose turi būti pateikti tikslūs paskelbimo pranešimai, pavadinimai, aprašai ir vaizdai ar vaizdo įrašai, susiję su programos funkcijomis ir (arba) turiniu, jos turi veikti patikimai ir tiksliai, kaip numatyta naudotojo.

Papildomus programos išteklius (pvz., žaidimo išteklius) galima atsisiųsti, tik jei jie reikalingi naudotojams norint naudoti programą. Atsisiųsti ištekliai turi atitikti visas „Google Play“ politikos nuostatas ir prieš pradėdant atsisiuntimo procesą programoje turi būti pateiktas raginimas naudotojams bei aiškiai nurodomas atsisiuntimo dydis.

Jei tvirtinama, kad programa sukurta norint pajuokauti ar pasilinksinti (ar kitu panašiu tikslu), programai vis tiek taikomos šios politikos nuostatos.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Programos, kurios imituoja kitas programas ar svetaines, kad apgaule priverstų naudotojus atskleisti asmens ar autentifikavimo informaciją.
- Programos, kuriose vaizduojami ar pateikiami asmenų ar subjektų nepatvirtinti ar realiame pasaulyje naudojami telefonų numeriai, kontaktinė informacija, adresai ar kita asmens identifikavimo informacija, negavus jų sutikimo.
- Programos su skirtingomis pagrindinėmis funkcijomis, pagrįstomis naudotojo geografinė vietoje, įrenginio parametrais ar kitais nuo naudotojų priklausančiais duomenimis, jei tie skirtumai nėra aiškiai reklamuojami naudotojui parduotuvės įrašė.
- Programos, kurių versijos pastebimai keičiasi neįspėjus naudotojo (pvz., [naujienų skyriuje](#)) ir neatnaujinus parduotuvės įrašė.
- Programos, kurios peržiūros metu bando pakeisti arba klaidinti elgseną.
- Programos, kurių atsisiuntimai vykdomi per turinio pateikimo tinklą (TPT) ir kuriose prieš atsisiunčiant nepateikiamas raginimas naudotojams ir nenurodomas atsisiuntimo dydis.

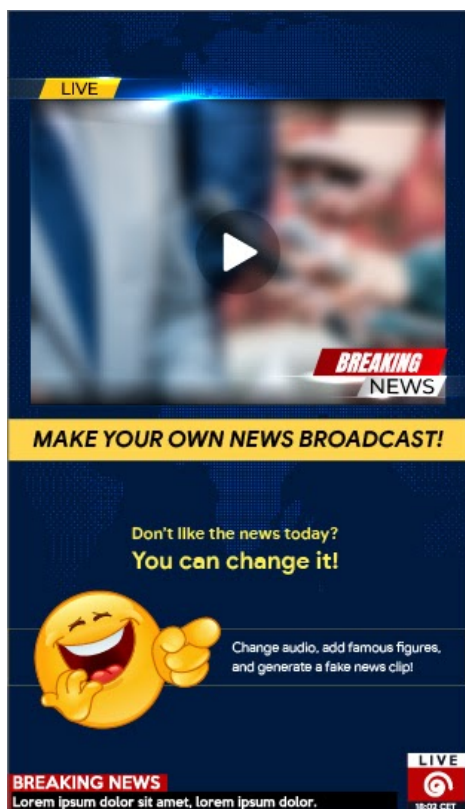
Manipuliuojama medija

Neleidžiame programų, reklamuojančių ar padedančių kurti apgaulingą ar klaidinančią informaciją arba tvirtinimus, perteikiamus per vaizdus, garsus, vaizdo įrašus ir (arba) tekstą. Neleidžiame programų, skirtų reklamuoti ar įamžinti aiškiai klaidinančius ar apgaulingus vaizdus, vaizdo įrašus ir (arba) tekstą, kurie gali būti žalingi, jei būtų naudojami nagrinėjant delikatių įvykių, politikos, socialines problemas ar kitus visuomenei rūpimus klausimus.

Programos, manipuliuojančios medija ar ją keičiančios (neįskaitant sutartinių ir redakcinių koregavimų, kad būtų aiškesnis ar kokybiškesnis turinys), turi aiškiai atskleisti ar vandens ženklų pažymėti pakeistą mediją, kai paprastam naudotojui gali būti neaišku, kad medija buvo pakeista. Išimtys gali būti taikomos, jei tai susiję su viešuoju interesu arba aišku, kad tai satyra ar parodija.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Programos, pridedančios viešą asmenį demonstracijoje per politinį renginį.
- Programos, naudojančios viešųjų asmenų duomenis ar mediją iš delikataus įvykio, kai siekiama reklamuoti medijos keitimo galimybes programos parduotuvės įrašė.
- Programos, keičiančios medijos klipus, siekiant pavaizduoti naujienų transliaciją.



1. Ši programa suteikia galimybę keisti medijos klipus, imituojančią naujienų transliaciją, ir prie klipo pridėti garsių ar viešų asmenų be vandens ženklo.

Elgsenos skaidrumas

Programos funkcijos turi būti visiškai aiškos naudotojams. Neįtraukite jokių paslėptų, neveikiančių ar dokumentuose nepateiktų funkcijų programoje. Neleidžiama taikyti programų peržiūros apėjimo metodų. Gali reikėti pateikti papildomos išsamios programų informacijos, siekiant užtikrinti naudotojų saugą, sistemos vientisumą ir politikos laikymąsi.

Klaidinantis pristatymas

Neleidžiame programų ar kūrėjų paskyrų, kuriose vykdoma toliau nurodyta veikla.

- Apsimetama kitu asmeniu ar organizacija arba klaidingai prisistatoma ar slepiama nuosavybės teisė arba pagrindinis tikslas.
 - Užsiimama koordinuota naudotojus klaidinančia veikla. Tai apima (bet tuo neapsiribojama) programas ar kūrėjų paskyras, kuriose netinkamai nurodoma ar slepiama jų kilmės šalis arba kuriose turinys nukreipiamas naudotojams kitoje šalyje.
 - Koordinuojami veiksmai su kitomis programomis, svetainėmis, kūrėjais ar kitomis paskyromis, siekiant nuslėpti ar klaidingai pristatyti kūrėjo ar programos tapatybę ar kitą išsamią medžiagos informaciją, kai programos turinys susijęs su politika, socialinėmis problemomis ar visuomenei aktualiais klausimais.
-

„Google Play“ tikslinio API lygio politika

Siekdama teikti naudotojams saugias ir patikimas funkcijas, „Google Play“ reikalauja toliau nurodytų tikslinių API lygių **visoms programoms**.

Visos naujos programos ir programų naujiniai TURI BŪTI taikomi pagal „Android“ API lygį per vienus metus nuo naujausios pagrindinės „Android“ OS versijos leidimo. Šio reikalavimo neatitinkančių programų ir programų naujinių bus neleidžiama teikti sistemoje „Play Console“.

Esamoms „Google Play“ programoms, kurios neatnaujintos ir kurios netaikomos pagal API lygį per dvejus metus nuo naujausio pagrindinio „Android“ versijos leidimo, bus nepasiekiamos naujiems naudotojams, naudojančiams įrenginius, kuriuose veikia naujesnių versijų „Android“ OS. Naudotojai, kurie anksčiau įdiegė programą iš „Google Play“, toliau galės surasti, iš naujo įdiegti ir naudoti programą bet kurios versijos „Android“ OS, kurią palaiko programa.

Jei reikia techninių patarimų, kaip įvykdyti tikslinio API lygio reikalavimą, žr. [perkėlimo vadovą](#).

Jei reikia tikslių terminų ir išimčių, žr. šį [pagalbos centro straipsnį](#).

SDK reikalavimai

Programų kūrėjai, norėdami integruoti pagrindines savo programų ir paslaugų funkcijas, dažnai naudojami trečiųjų šalių kodu (pvz., SDK). Įtraukdami SDK į savo programą, turite užtikrinti, kad galėsite garantuoti naudotojų saugumą ir apsaugoti programą nuo bet kokių pažeidimų. Šiame skyriuje pristatysime, kaip kai kurie mūsų esami privatumo ir saugos reikalavimai taikomi SDK kontekste ir yra skirti padėti kūrėjams saugiai ir patikimai integruoti SDK į savo programas.

Jei į savo programą įtraukiate SDK, esate atsakingi už tai, kad dėl jų trečiosios šalies kodo ir praktikos jūsų programa nepažeistų „Google Play“ kūrėjų programos politikos. Svarbu žinoti, kaip jūsų programoje esantys SDK tvarko naudotojų duomenis bei kokius leidimus jie naudoja, kokius duomenis renka ir kodėl. Atminkite, kad SDK naudotojų duomenys turi būti renkami ir tvarkomi laikantis jūsų programos politiką atitinkančios minėtų duomenų naudojimo tvarkos.

Norėdami užtikrinti, kad SDK naudojimas nepažeistų politikos reikalavimų, perskaitykite ir supraskite visą toliau pateiktą politiką ir atkreipkite dėmesį į kai kuriuos esamus reikalavimus, susijusius su SDK.

Naudotojų duomenų politika

Turite aiškiai nurodyti, kaip apdorojate naudotojo duomenis (pvz., iš naudotojo arba apie jį surinktą informaciją, įskaitant įrenginio informaciją). Tai reiškia, kad reikia atskleisti, kaip pasiekiate, renkate, naudojate, tvarkote ir bendrinatė programos naudotojo duomenis, bei apriboti duomenų naudojimą pagal duomenų atskleidimo politikos reikalavimus.

Jei į programą įtraukiate trečiosios šalies kodą (pvz., SDK), privalote užtikrinti, kad programoje naudojamas trečiosios šalies kodas ir tos trečiosios šalies veiksmai, susiję su programoje esančiais naudotojo duomenimis, atitiktų „Google Play“ kūrėjų programos politiką, įskaitant naudojimo ir atskleidimo reikalavimus. Pavyzdžiui, turite užtikrinti, kad SDK teikėjai neparduotų asmens ir neskelbtinų programos naudotojų duomenų. Šis reikalavimas taikomas neatsižvelgiant į tai, ar naudotojo duomenys perduodami juos nusiuntus į serverį, ar į programą įterpiant trečiosios šalies kodą.

Asmens ir neskelbtini naudotojo duomenys

- Iš programos gautus asmens ir neskelbtinus naudotojų duomenis pasiekti, rinkti, naudoti ir bendrinti galima tik siekiant teikti programos ir paslaugų funkcijas bei laikytis politikos, ko pagrįstai tikisi naudotojas:
 - programos, kuriose asmens ir neskelbtini naudotojo duomenys naudojami reklamai rodyti, turi atitikti „Google Play“ skelbimų politiką;
- turite saugiai tvarkyti visus asmens ir neskelbtinus naudotojo duomenis, įskaitant jų perdavimą, naudodami modernią kriptografiją (pvz., per HTTPS);
- turite naudoti vykdymo laiko leidimų užklausą (kai pasiekama), prieš pasiekdami duomenis, kuriems taikomi „Android“ leidimai.

Asmens ir neskelbtinų naudotojų duomenų pardavimas

Neparduokite asmens ir neskelbtinų naudotojo duomenų.

- Pardavimas yra keitimasis asmens ir neskelbtiniais naudotojo duomenimis arba jų perdavimas trečiajai šaliai už piniginį atlygį.

- Naudotojo inicijuotas asmens ir neskelbtinų naudotojo duomenų perdavimas (pavyzdžiui, kai naudotojas, naudodamas programos funkciją, perduoda failą trečiajai šaliai ar nusprendžia naudoti specialios paskirties mokslinių tyrimų programą) nelaikomas pardavimu.

Aiškaus paskelbimo ir sutikimo reikalavimai

Jei jūsų programos prieiga prie asmens ir neskelbtinų naudotojo duomenų, jų rinkimas, naudojimas ar bendrinimas gali neatitikti pagrįstų atitinkamo produkto ar funkcijos naudotojo lūkesčių, privalote laikytis [naudotojų duomenų politikos](#) aiškaus paskelbimo ir sutikimo reikalavimų.

Jei programoje integruotas trečiosios šalies kodas (pvz., SDK), kuris pagal numatytuosius nustatymus yra skirtas rinkti asmens ir neskelbtinų naudotojo duomenis, per dvi savaites nuo „Google Play“ užklauso gavimo (arba, jei „Google Play“ užklausoje numatytas ilgesnis laikotarpis, per tą laikotarpį) turite pateikti pakankamai įrodymų, kad programa atitinka šios politikos aiškaus paskelbimo ir sutikimo reikalavimus, įskaitant susijusius su prieiga prie duomenų, jų rinkimu, naudojimu ar bendrinimu naudojant trečiosios šalies kodą.

Nepamirškite, kad turite užtikrinti, jog dėl naudojamo trečiosios šalies kodo (pvz., SDK) programa nepažeistų [naudotojų duomenų politikos](#).

Jei reikia daugiau informacijos apie aiškaus paskelbimo ir sutikimo reikalavimą, žr. šį [pagalbos centro](#) straipsnį.

SDK sukeltų pažeidimų pavyzdžiai

- Programa su SDK, kuri renka asmens ir neskelbtinų naudotojo duomenis ir šiems duomenims netaiko šios naudotojų duomenų politikos, prieigos, duomenų tvarkymo (įskaitant neleistiną pardavimą) ir aiškaus paskelbimo ir sutikimo reikalavimų.
- Programoje integruotas SDK, kuris pagal numatytuosius nustatymus renka asmeninius ir neskelbtinų naudotojo duomenis, pažeidžiant šios politikos reikalavimus dėl naudotojo sutikimo ir aiškaus atskleidimo.
- Programa su SDK, kurioje teigiama, kad asmens ir neskelbtini naudotojų duomenys renkami tik tam, kad būtų užtikrinamos programos kovos su sukčiavimu ir piktnaudžiavimu funkcijos, tačiau SDK taip pat dalijasi surinktais duomenimis su trečiosiomis šalimis reklamai ar analizei.
- Programoje yra SDK, kuris perduoda naudotojų įdiegtus informacijos paketus nesilaikant aiškaus paskelbimo gairių ir (arba) [privatumo politikos gairių](#).
 - Taip pat žr. [mobiliesiems skirtos nepageidaujamos programinės įrangos](#) politiką.

Papildomi reikalavimai prieigai prie asmens ir neskelbtinų duomenų

Toliau pateiktoje lentelėje aprašomi konkrečiai veiklai taikomi reikalavimai.

Veikla	Reikalavimas
Programoje renkami arba susiejami nuolatiniai įrenginio identifikatoriai (pvz., IMEI, IMSI, SIM serijos numeris ir pan.)	Nuolatinį įrenginio identifikatorių negalima susieti su kitais asmens ir neskelbtiniais naudotojų duomenimis arba iš naujo nustatoma įrenginio identifikatoriais, išskyrus atvejus, kai tai būtina norint teikti: • telefonijos paslaugas, susietas su SIM kortelės tapatybės nustatymu (pvz., „Wi-Fi“ skambinimo, susieto su operatoriaus paskyra, paslaugas), ir • įmonių įrenginių tvarkymo programas, kuriose naudojamas įrenginio savininko režimas. Apie tokį naudojimą turi būti aiškiai paskelbta naudotojams, kaip nurodyta naudotojų duomenų politikoje. Daugiau informacijos apie alternatyvius unikalius identifikatorius rasite šiame šaltinyje. Norėdami gauti papildomos informacijos apie „Android“ reklamavimo ID, perskaitykite skelbimų politiką.
Programa taikoma vaikams	Jūsų programoje gali būti tik tie SDK, kurie yra savarankiškai sertifikuoti vaikams skirtose paslaugose. Visą politikos tekstą ir reikalavimus žr. savarankiškai sertifikuotų skelbimų SDK programoje šeimoms.

SDK sukeltų pažeidimų pavyzdžiai

- Programoje naudojamas SDK, susiejantis su „Android“ ID su vietove.
- Programa su SDK, kuris susieja AAID su nuolatiniais įrenginio identifikatoriais, kad būtų galima reklamuoti ar atlikti analizę.
- Programoje naudojamas SDK, susiejantis AAID su el. pašto adresu analizei atlikti.

Skiltis „Duomenų sauga“

Visi kūrėjai turi pateikti aiškią ir tikslią informaciją kiekvienos programos „Duomenų saugos“ skiltyje, kurioje išsamiai apibūdinamas naudotojų duomenų rinkimas, naudojimas ir bendrinimas. Tai taip pat taikoma duomenims, kurie renkami ir tvarkomi naudojant bet kokias trečiųjų šalių bibliotekas ar jų programose esančius SDK. Kūrėjas yra atsakingas už privatumo etiketės tikslumą ir joje pateikiamos informacijos atnaujinimą. Jei reikalaujama, skiltyje pateikta informacija turi atitikti programos privatumo politikoje pateiktus paskelbimus.

Jei reikia papildomos informacijos apie skilties „Duomenų sauga“ pildymą, žr. šį [pagalbos centro](#) straipsnį.

Žr. visą [naudotojų duomenų politiką](#).

Leidimai ir API, kurie pasiekia neskelbtinos informacijos politiką

Leidimų ir API, kurie pasiekia neskelbtiną informaciją, užklauskos turi būti suprantamos naudotojams. Galite pateikti užklausą tik dėl tų neskelbtiną informaciją pasiekiančių leidimų ir API, kurie yra būtini norint įdiegti esamas programos funkcijas ar paslaugas, reklamuojamas „Google Play“ įrašė. Negalite naudoti leidimų ar API, kurie pasiekia neskelbtiną informaciją ir kuriais leidžiama pasiekti naudotojo ar įrenginio duomenis dėl neatskleistų, neįdiegtų ar neleistinių funkcijų arba tokiais tikslais. Asmens ar neskelbtini duomenys, pasiekiami per leidimus ar API, kurie pasiekia neskelbtiną informaciją, niekada negali būti parduodami ar bendrinami, siekiant palengvinti pardavimą.

Žr. visą [leidimų ir API, kurie pasiekia neskelbtiną informaciją, politiką](#).

SDK sukeltų pažeidimų pavyzdžiai

- Jūsų programoje yra SDK, kuris teikia įrenginio vietovės užklauskas fone neleistinu ar neatskleistu tikslu.
- Jūsų programoje yra SDK, kuris perduoda IMEI, gautą iš „Android“ leidimo „read_phone_state“ be naudotojo sutikimo.

Kenkėjiškų programų politika

Mūsų kenkėjiškų programų politika paprasta: „Android“ ekosistemoje, įskaitant „Google Play“ parduotuvę ir naudotojų įrenginius, negali būti kenkėjiškos elgsenos (t. y. kenkėjiškų programų). Laikydami šio pagrindinio principo stengiamės užtikrinti saugią „Android“ ekosistemą naudotojams ir jų „Android“ įrenginiams.

Kenkėjiška programa – tai bet koks kodas, dėl kurio gali kilti pavojus naudotojui, jo duomenims ar įrenginiui. Kenkėjiškos programos apima (bet tuo neapsiribojama) potencialiai žalingas programas (PŽP), dvejetaines programas arba struktūrų pakeitimus, apimančius tokias kategorijas kaip Trojos arkliai, sukčiavimo ir šnipinėjimo programos. Be to, nuolat atnaujiname ir pridedame naujų kategorijų.

Šios politikos reikalavimai taip pat taikomi bet kokiam trečiosios šalies kodui (pvz., SDK), kurį įtraukiate į savo programą.

Žr. visą [kenkėjiškų programų politiką](#).

SDK sukeltų pažeidimų pavyzdžiai

- Programa, kurioje yra kenkėjišką programinę įrangą platinančių teikėjų SDK bibliotekų.
- Programa, pažeidžianti „Android“ modelį arba vagianti prisijungimo duomenis (pvz., „OAuth“ prieigos raktus) iš kitų programų.
- Programos, piktnaudžiaujančios funkcijomis, kai neleidžiama jų pašalinti ar sustabdyti.
- „SELinux“ išjungianti programa.

- Programa, kurioje yra SDK, kuris pažeidžia „Android“ leidimų modelį, nes įgyja aukštesnio lygio privilegijas, suteikdamas prieigą prie įrenginio duomenų neatskleistu tikslu.
- Programa, kurioje yra SDK su kodu, kuriuo naudotojai apgaulės būdu verčiami prenumeruoti arba pirkti turinį per savo mobiliojo telefono sąskaitą.

Privilegijų išplėtimo programos, kurios be naudotojo leidimo įgalina prieigą prie šakninio įrenginių katalogo, laikomos prieigą prie šakninio katalogo įgalinančiomis programomis.

Šnipinėjimo programa

Šnipinėjimo programa yra kenkėjiška programa, kodas ar elgsena, kurią naudojant renkami, gaunami ar bendrinami naudotojo arba įrenginio duomenys, nesusiję su politiką atitinkančiomis funkcijomis.

Kenkėjiškas kodas ar elgsena, kuriuos galima laikyti naudotojo šnipinėjimu arba kuriuos naudojant renkami duomenys tinkamai nepranešus ir negavus sutikimo, taip pat vadinami šnipinėjimo programa.

Žr. visą [šnipinėjimo programų politiką](#).

Toliau pateikiama šnipinėjimo programų, kuriose naudojamas SDK, pavyzdžių (sąrašas nėra baigtinis).

- Programa, kurioje naudojamas SDK, perduodantis duomenis iš garso arba skambučių įrašų, kai tai nėra susiję su politiką atitinkančiomis programos funkcijomis.
- Programa su kenkėjišku trečiosios šalies kodu (pvz., SDK), perduodanti įrenginio duomenis būdu, kurio naudotojas nesitiki, ir (arba) tinkamai nepranešus naudotojui ir negavus naudotojo sutikimo.

Mobiliesiems skirtos nepageidaujamos programinės įrangos politika

Skaidri elgsena ir aiškūs paskelbimai

Visas kodas turi atitikti naudotojui pateiktus pažadus. Programose turėtų būti teikiamos visos nurodytos funkcijos. Programos neturėtų klaidinti naudotojų.

Toliau pateikiama pažeidimų pavyzdžių.

- Apgaulingi skelbimai
- Socialinė inžinerija

Naudotojo duomenų apsauga

Aiškiai ir išsamiai nurodykite prieigą prie asmens ir neskelbtinų naudotojų duomenų, jų naudojimą, rinkimą ir bendrinimą. Naudotojų duomenų naudojimas turi atitikti visą atitinkamą naudotojų duomenų politiką (jei taikoma) ir turi būti imamas visų atsargumo priemonių duomenims apsaugoti.

Toliau pateikiama pažeidimų pavyzdžių.

- Duomenų rinkimas (palyginti su šnipinėjimo programa)
- Piktnaudžiavimas ribotais leidimais

Žr. visą [mobiliesiems skirtos nepageidaujamos programinės įrangos politiką](#)

Piktnaudžiavimo įrenginiu ir tinklu politika

Neleidžiame teikti programų, kurios neteisėtai trikdo, pažeidžia ar pasiekia naudotojo įrenginį, kitus įrenginius ar kompiuterius, serverius, tinklus, programų programavimo sąsajas (API) ar paslaugas, įskaitant (bet tuo neapsiribojant) kitas įrenginyje esančias programas, bet kokią „Google“ paslaugą ar įgaliojotojo teikėjų tinklą.

Programos ar trečiosios šalies kodas (pvz., SDK) su interpretuojamomis kalbomis („JavaScript“, „Python“, „Lua“ ir pan.), įkeliami paleidžiant (pvz., neįtraukti į programos paketą), negali kelti „Google Play“ politikos nuostatų pažeidimo rizikos.

Neleidžiame naudoti kodo, kuriame yra saugos pažeidimų. Peržiūrėkite [programų saugumo tobulinimo paslaugą](#) ir sužinokite apie naujausias saugos problemas, apie kurias pranešta kūrėjams.

Žr. visą [piktnaudžiavimo įrenginiu ir tinklu politiką](#).

SDK sukeltų pažeidimų pavyzdžiai

- Programos, trečiosioms šalims palengvinančios naudojimąsi tarpinio serverio paslaugomis, gali tai daryti tik tokiu atveju, jei tai yra pagrindinė ir svarbiausia naudotojui teikiama programos funkcija.
- Jūsų programoje yra SDK, kuris atsisiunčia vykdomąjį kodą, pvz., „dex“ failus arba savąjį kodą, iš kito šaltinio nei „Google Play“.
- Į programą įtrauktas SDK, apimantis žiniatinklio rodinį su pridėta „JavaScript“ sąsaja, įkeliančia nepatiktą žiniatinklio turinį (pvz., http:// URL) arba nepatvirtintus URL, gautus iš nepatiktų šaltinių (pvz., URL, gautus su nepatikimais tikslais).
- Jūsų programoje yra SDK, kuriame yra kodas, naudotas savo APK naujinti.
- Jūsų programoje yra SDK, dėl kurio pažeidžiamas naudotojų saugumas atsisiunčiant failus nesaugiu ryšiu.
- Jūsų programoje naudojamas SDK, kuriame yra kodas, skirtas programoms atsisiųsti ar įdiegti iš nežinomų šaltinių už sistemos „Google Play“ ribų.
- Į programą įtrauktas SDK, naudojantis priekinio plano paslaugas be atitinkamo naudojimo atvejo.
- Į programą įtrauktas SDK, naudojantis priekinio plano paslaugas, kad būtų laikomasi politikos nuostatų, bet tai neapibrėžta programos apraše.

Apgaulingos elgsenos politika

Neleidžiame teikti programų, kuriose bandoma apgauti naudotojus ar įgalinti nesąžiningą elgesį, įskaitant programas (bet jomis neapsiribojant), kurių funkcijos negali būti vykdomos. Programose turi būti pateiktas tikslus jos funkcijų paskelbimo pranešimas, aprašas ir vaizdai / vaizdo įrašai visose metaduomenų dalyse. Programose negali būti kopijuojamos funkcijos ar įspėjimai iš operacinės sistemos ar kitų programų. Bet kokie įrenginio nustatymų pakeitimai turi būti atliekami pranešus naudotojui ir gavus jo sutikimą ir jie turi būti grąžinami.

Žr. visą [apgaulingos elgsenos politiką](#).

Elgsenos skaidrumas

Programos funkcijos turi būti visiškai aiškios naudotojams. Neįtraukite jokių paslėptų, neveikiančių ar dokumentuose nepateiktų funkcijų programoje. Neleidžiama taikyti programų peržiūros apėjimo metodų. Gali reikėti pateikti papildomos išsamios programų informacijos, siekiant užtikrinti naudotojų saugą, sistemos vientisumą ir politikos laikymąsi.

Pažeidimo, susijusio su SDK, pavyzdys

- Jūsų programoje yra SDK, kuriame naudojami programų apžvalgų vengimo metodai.

Kuri „Google Play“ politika programų kūrėjams dažniausiai siejama su SDK sukeltais pažeidimais?

Siekiant užtikrinti, kad visi jūsų programos naudojami kodai atitiktų „Google Play“ kūrėjų programos politiką, žr. visą toliau pateiktą politiką.

- [Naudotojų duomenų politika](#)
- [Leidimai ir API, kurie pasiekia neskelbtiną informaciją](#)
- [Piktnaudžiavimo įrenginiu ir tinklu politika](#)
- [Kenkėjiška programa](#)
- [Mobiliesiems skirta nepageidaujama programinė įranga](#)
- [Savarankiškai sertifikuotų skelbimų SDK programa šeimoms](#)
- [Skelbimų politika](#)

- [Apgaulinga elgsena](#)
- [„Google Play“ kūrėjų programos politika](#)

Nors su šiomis politikomis susiduriama dažniausiai, svarbu nepamiršti, kad dėl blogo SDK kodo jūsų programa gali pažeisti kitą, pirmiau nepamintą politiką. Nepamirškite peržiūrėti ir nuolat sekti visų politikos naujienų, nes jūs, kaip programų kūrėjas, privalote užtikrinti, kad jūsų SDK tvarkytų jūsų programos duomenis laikantis taisyklių.

Norėdami sužinoti daugiau, apsilankykite [pagalbos centre](#).

Kenkėjiška programa

Mūsų kenkėjiškų programų politika paprasta: „Android“ ekosistemoje, įskaitant „Google Play“ parduotuvę ir naudotojų įrenginius, negali būti kenkėjiškos elgsenos (t. y. kenkėjiškų programų). Laikydami šio pagrindinio principo stengiamės užtikrinti saugią „Android“ ekosistemą naudotojams ir jų „Android“ įrenginiams.

Kenkėjiška programa – tai bet koks kodas, dėl kurio gali kilti pavojus naudotojui, jo duomenims ar įrenginiui. Kenkėjiškos programos apima (bet tuo neapsiribojama) potencialiai žalingas programas (PŽP), dvejetaines programas arba struktūrų pakeitimus, apimančius tokias kategorijas kaip Trojos arkliai, sukčiavimo ir šnipinėjimo programos. Be to, nuolat atnaujiname ir pridedame naujų kategorijų.

Šios politikos reikalavimai taip pat taikomi bet kokiam trečiosios šalies kodui (pvz., SDK), kurį įtraukiate į savo programą.

Nors skiriasi kenkėjiškų programų tipai ir funkcijos, įprastai jų tikslas yra vienas iš nurodytų.

- Pažeisti naudotojo įrenginio vientisumą.
- Perimti naudotojo įrenginio valdymą.
- Įgalinti nuotoliniu būdu valdomas operacijas, kad atakos vykdytojas galėtų pasiekti, naudoti ar kitais būdais išnaudoti pažeistą įrenginį.
- Perduoti asmens arba prisijungimo duomenis iš įrenginio be atitinkamo paskelbimo pranešimo ir sutikimo.
- Platinti šlamštą ar komandas iš pažeisto įrenginio, siekiant paveikti kitus įrenginius ar tinklus.
- Apgauti naudotoją.

Programa, dvejetainė programa ar struktūros pakeitimas gali būti potencialiai žalingas ir atitinkamai generuoti kenkėjišką elgseną, net jei tai nebuvo numatyta. Taip gali nutikti, nes programos, dvejetainės programos ar struktūros pakeitimai gali veikti kitaip, atsižvelgiant į įvairius kintamuosius. Todėl tai, kas žalinga vienam „Android“ įrenginiui, gali nesukelti pavojaus kitam „Android“ įrenginiui. Pvz., įrenginiui, kuriame vykdoma naujausios versijos „Android“, neturi įtakos žalingos programos, naudojančios nebenaudojamas API kenkėjiškiems veiksams atlikti, bet pavojus gali kilti įrenginiui, kuriame vis dar vykdoma labai senos versijos „Android“. Programos, dvejetainės programos arba struktūros pakeitimai pažymimi kaip kenkėjiškos programos arba PŽP, jei jos aiškiai kelia pavojų kai kuriems arba visiems „Android“ įrenginiams ir naudotojams.

Toliau nurodytos kenkėjiškų programų kategorijos atspindi mūsų pagrindinį principą, kad naudotojai turėtų suprasti, kaip jų įrenginys naudojamas, ir skatinti saugią ekosistemą, įgalinančią veiksmingas naujoves ir patikimas naudotojams teikiamas funkcijas.

Jei reikia daugiau informacijos, apsilankykite [„Google Play Protect“](#).

Užpakalinės durys

Kodas, kurį naudojant galima vykdyti nepageidaujamas, potencialiai žalingas, nuotoliniu būdu valdomas operacijas įrenginyje.

Šios operacijos gali apimti elgseną, dėl kurios programos, dvejetainės programos ar struktūros pakeitimas būtų priskirtas vienai iš kitų kenkėjiškų programų kategorijų, jei būtų vykdoma automatiškai.

Apskritai, terminu „užpakalinės durys“ apibrėžiama, kaip gali įvykti potencialiai žalinga operacija įrenginyje, todėl tai ne visiškai atitinka tokias kategorijas kaip apgaulingas atsiskaitymas ar komercinės šnipinėjimo programos. Todėl esant tam tikroms aplinkybėms užpakalinių durų poaibį „Google Play Protect“ laiko pažeidimu.

Apgaulingas atsiskaitymas

Kodas, kurį naudojant naudotojas automatiškai apmokestinamas, siekiant apgauti.

Apgaulingi atsiskaitymo per mobiliojo ryšio operatorių metodai skirstomi į apgaulingus SMS, apgaulingus skambučius ir apgaulingas mokamas paslaugas.

Apgaulingi SMS

Kodas, kurį naudojant naudotojai apmokestinami siunčiant mokamus SMS be sutikimo arba bandoma slėpti SMS veiklą slepiant mobiliojo ryšio operatoriaus paskelbimo sutartis ar SMS pranešimus, kuriais naudotojas informuojamas apie mokesčius ar kuriais patvirtinamos prenumeratos.

Tam tikru kodu atliekami papildomi su apgaulingais SMS susiję veiksmai, nors techniškai skelbiama SMS siuntimo elgsena. Pavyzdžiai: slepiamos paskelbimo sutarties dalys nuo naudotojo, jos padaromos neįskaitomos ir atsižvelgiant į aplinkybes slepiami mobiliojo ryšio operatoriaus SMS pranešimai, kuriais naudotojas informuojamas apie mokesčius arba kuriais patvirtinama prenumerata.

Apgaulingi skambučiai

Kodas, kurį naudojant naudotojai apmokestinami skambinant mokamais numeriais be naudotojo sutikimo.

Apgaulingos mokamos paslaugos

Kodas, kurį naudojant naudotojai apgaule priverčiami prenumeruoti ar įsigyti turinio, kurio mokestis įtraukiamas į mobiliojo telefono sąskaitą.

Apgaulingos mokamos paslaugos apima bet kokio tipo atsiskaitymą, išskyrus mokamus SMS ir mokamus skambučius. Pavyzdžiai: tiesioginis atsiskaitymas per operatorių, belaidis prieigos taškas (WAP) ir mobiliojo ryšio mokesčio perkėlimas. WAP apgaulės metodas yra vienas iš labiausiai paplitusių apgaulingų mokamų paslaugų tipų. Taikant WAP apgaulės metodą naudotojai gali būti apgaule priverčiami spustelėti mygtuką nepastebimai įkeltame, skaidriame žiniatinklio rodinyje. Atlikus veiksmą inicijuojama pasikartojanti prenumerata, o patvirtinimo SMS arba el. laiškas dažnai užgrobiamas, kad naudotojai nepastebėtų finansinės operacijos.

Stebėjimo programa

Kodas, kurį naudojant renkami asmens ar neskelbtini naudotojo duomenys iš įrenginio ir perduodami duomenys trečiajai šaliai (įmonei ar kitam fiziniam asmeniui) stebėjimo tikslais.

Programose turi būti pateiktas tinkamas aiškus paskelbimas ir gautas sutikimas, kaip reikalaujama pagal [naudotojų duomenų politiką](#).

Stebėjimo programų gairės

Priimtinos tik tokios stebėjimo programos, kurios yra išimtinai skirtos kitam fiziniam asmeniui stebėti, pvz., tėvams, kad galėtų stebėti vaikus, ar įmonei valdyti, norint stebėti atskirus darbuotojus, ir tokiu tikslu reklamuojamos. Jos turi visiškai atitikti toliau nurodytus reikalavimus. Šios programos negali būti naudojamos kitam asmeniui (pvz., sutuoktiniui) stebėti net su jo žinia ir leidimu, jei nerodomas nuolatinis pranešimas. Šių programų aprašo faile turi būti naudojama „IsMonitoringTool“ metaduomenų žyma, kad būtų tinkamai priskirtos stebėjimo programoms.

Stebėjimo programos turi atitikti toliau nurodytus reikalavimus.

- Programos neturi nurodyti, kad yra šnipinėjimo arba slaptos stebėjimo priemonės.
- Programos negali slėpti ar pridengti stebėjimo funkcijų arba bandyti klaidinti naudotojus apie tokias funkcijas.

- Programai veikiant, privaloma naudotojams visada rodyti nuolatinį pranešimą ir unikalią piktogramą, kuri aiškiai identifikuoja programą.
- Programų stebėjimo funkcijos turi būti paskelbtos jų „Google Play“ parduotuvės apraše.
- Programose ir programų įrašuose sistemoje „Google Play“ negalima teikti būdų, kaip suaktyvinti ar pasiekti funkcijas, kurios pažeidžia šias sąlygas, pvz., susieti su reikalavimų neatitinkančiu APK, kuris priglobiamas ne sistemoje „Google Play“.
- Programose būtina laikytis visų galiojančių įstatymų. Tik jūs patys atsakote už savo programos teisėtumo tikslinėje jos naudojimo lokalėje nustatymą.

Peržiūrėkite pagalbos centro straipsnį „[isMonitoringTool“ žymos naudojimas](#)“, jei reikia daugiau informacijos.

Aptarnavimo perkrova (DoS)

Kodas, kuriuo, nežinant naudotojui, vykdoma aptarnavimo perkrovos („DoS“) ataka arba kuris naudojamas vykdant paskirstytą „DoS“ ataką prieš kitas sistemas ir šaltinius.

Pvz., tai gali būti atliekama siunčiant labai daug HTTP užklausų siekiant labai apkrauti nuotolinius serverius.

Kenkėjiškos atsisiuntimo programos

Kodas, kuris nėra potencialiai žalingas, bet jį naudojant atsisiunčiama kitų PŽP.

Kodas gali veikti kaip kenkėjiška atsisiuntimo programa, jei:

- galima pagrįstai manyti, kad jis buvo sukurtas siekiant platinti PŽP ir jį naudojant buvo atsisiųsta PŽP arba jis apima kodą, kurį naudojant galima atsisiųsti ir įdiegti programas; arba
- mažiausiai 5 proc. jį naudojant atsisiųstų programų yra PŽP, kai minimalus stebimų programų atsisiuntimų slenkstis yra 500 (25 stebimi PŽP atsisiuntimai).

Pagrindinės naršyklės ir failų bendrinimo programos nėra laikomos kenkėjiškomis atsisiuntimo programomis, jei:

- jos neskatina atsisiuntimų naudotojui neatliekant veiksmų ir
- visi PŽP atsisiuntimai vykdomi gavus naudotojų sutikimą.

Ne „Android“ grėsmė

Kodas, apimantis ne „Android“ grėsmes.

Šios programos negali pakenkti „Android“ naudotojui arba įrenginiui, bet jose gali būti komponentų, kurie gali būti žalingi kitoms platformoms.

Sukčiavimas

Naudojant kodą, kuris apgaulingai nurodomas kaip pateiktas iš patikimo šaltinio, teikiama naudotojo autentifikavimo prisijungimo duomenų ar atsiskaitymo informacijos užklausa ir siunčiami duomenys trečiajai šaliai. Ši kategorija taip pat taikoma kodui, kuriuo perimamas naudotojo prisijungimo duomenų perdavimas.

Dažniausiai sukčiaujama siekiant gauti bankininkystės prisijungimo duomenis, kredito kortelių numerius ir socialinių tinklų bei žaidimų internetinių paskyrų prisijungimo duomenis.

Piktnaudžiavimas aukštesnio lygio privilegijomis

Kodas, kurį taikant pažeidžiamas sistemos vientisumas, pažeidžiant programos smėlio dėžę, gaunant aukštesnio lygio privilegijų ar keičiant arba išjungiant prieigą prie pagrindinių su sauga susijusių funkcijų.

Pavyzdžiai

- Programa, pažeidžianti „Android“ modelį arba vagianti prisijungimo duomenis (pvz., „OAuth“ prieigos raktus) iš kitų programų.
- Programos, piktnaudžiaujančios funkcijomis, kai neleidžiama jų pašalinti ar sustabdyti.
- „SELinux“ išjungianti programa.

Privilegijų išplėtimo programos, kurios be naudotojo leidimo įgalina prieigą prie šakninio įrenginių katalogo, laikomos prieigą prie šakninio katalogo įgalinančiomis programomis.

Išpirkos reikalaujanti programinė įranga

Kodas, kurį taikant iš dalies arba visiškai valdomas įrenginys arba įrenginio duomenys ir reikalaujama, kad naudotojas sumokėtų ar atliktų veiksmą kontrolės funkcijoms pašalinti.

Tam tikra išpirkos reikalaujanti programinė įranga šifruoja duomenis įrenginyje ir reikalauja mokėjimo, kad būtų iššifruoti duomenys, ir (arba) naudoja administratoriaus funkcijas, kad programos negalėtų pašalinti įprastas naudotojas. Pavyzdžiai

- Naudotojui neleidžiama naudoti įrenginio ir reikalaujama sumokėti, kad būtų atkurta naudotojo kontrolė.
- Šifruojami įrenginio duomenys ir reikalaujama sumokėti, kad tariamai būtų iššifruoti duomenys.
- Perimamos įrenginio politikos tvarkyklės funkcijos ir naudotojui neleidžiama pašalinti programos.

Su įrenginiu platinamas kodas, kurio pagrindinis tikslas yra subsidijuotas įrenginio valdymas, gali būti neįtrauktas į išpirkos reikalaujančios programinės įrangos kategoriją, jei jis atitinka saugaus užrakimo ir valdymo reikalavimus ir atitinkamus paskelbimo naudotojams ir jų sutikimo reikalavimus.

Prieigos prie šakninio katalogo įgalinimas

Prieigą prie šakninio įrenginio katalogo įgalinantis kodas.

Ne kenkėjiški ir kenkėjiški prieigos prie šakninio katalogo įgalinimo kodai skiriasi. Pvz., naudojant ne kenkėjiškas prieigos prie šakninio katalogo įgalinimo programas naudotojui iš anksto pranešama, kad ketinama įgalinti prieigą prie šakninio įrenginio katalogo, ir jos nevykdo kitų potencialiai žalingų veiksmų, priskiriamų kitoms PŽP kategorijoms.

Naudojant kenkėjiškas prieigos prie šakninio katalogo įgalinimo programas naudotojas nėra informuojamas apie būsimą prieigos prie šakninio įrenginio katalogo įgalinimą arba naudotojui iš anksto pranešama apie prieigos prie šakninio katalogo įgalinimą, bet taip pat vykdomi kiti veiksmai, kurie priskiriami kitoms PŽP kategorijoms.

Šlamštas

Kodas, kurį taikant siunčiami nepageidaujami pranešimai naudotojo kontaktams arba įrenginys naudojamas el. pašto šlamštui perduoti.

Šnipinėjimo programa

Šnipinėjimo programa yra kenkėjiška programa, kodas ar elgsena, kurią naudojant renkami, gaunami ar bendrinami naudotojo arba įrenginio duomenys, nesusiję su politiką atitinkančiomis funkcijomis.

Kenkėjiškas kodas ar elgsena, kuriuos galima laikyti naudotojo šnipinėjimu arba kuriuos naudojant renkami duomenys tinkamai nepranešus ir negavus sutikimo, taip pat vadinami šnipinėjimo programa.

Toliau pateikiama šnipinėjimo programų pavyzdžių (sąrašas nėra baigtinis).

- Garso ar telefono skambučių įrašymas.
- Programos duomenų vagystė.

- Programa su kenkėjišku trečiosios šalies kodu (pvz., SDK), perduodanti įrenginio duomenis būdu, kurio naudotojas nesitiki, ir (arba) tinkamai nepranešus naudotojui ir negavus naudotojo sutikimo.

Be to, visos programos turi atitikti visas „Google Play“ kūrėjų programos politikos nuostatas, įskaitant naudotojo ir įrenginio duomenų politiką, pvz., [mobiliesiems skirtos nepageidaujamos programinės įrangos](#), [naudotojo duomenų](#), [leidimų ir API](#), [pasiekiančių neskelbtiną informaciją](#), bei [SDK reikalavimus](#).

Trojos arklys

Kodas, kuris atrodo paprastas, pvz., žaidimas, kai tvirtinama, kad tai tik žaidimas, bet kurį taikant atliekami nepageidaujami veiksmai kenkiant naudotojui.

Ši klasifikacija įprastai naudojama kartu su kitomis PŽP kategorijomis. Trojos arklys apima nekenksmingą komponentą ir paslėptą žalingą komponentą. Pvz., žaidimas, fone siunčiantis mokamus SMS pranešimus iš naudotojo įrenginio jam to nežinant.

Pastaba apie neįprastas programas

Naujos ir retos programos gali būti priskiriamos neįprastų programų kategorijai, jei „Google Play Protect“ neturi pakankamai informacijos, patvirtinančios jų saugumą. Tai nereiškia, kad programa tikrai žalinga, bet ir negalima teigti, kad ji saugi, išsamiau neperžiūrėjus.

Pastaba dėl užpakalinių durų kategorijos

Užpakalinių durų kenkėjiškos programos kategorija klasifikuojama pagal kodo veiksmus. Būtina bet kokio kodo priskyrimo užpakalinių durų kategorijai sąlyga yra elgsenos, dėl kurios kodas būtų priskirtas vienai iš kitų kenkėjiškų programų kategorijų, jei būtų vykdomas automatiškai, įgalinimas. Pvz., jei programa leidžia dinamiškai įkelti kodą, o dinamiškai įkeltas kodas renka teksto pranešimus, programa priskiriama užpakalinių durų kenkėjiškų programų kategorijai.

Tačiau, jei programa leidžia kenksmingai vykdyti kodą ir nėra jokių priežasčių manyti, kad šis kodas vykdomas siekiant atlikti kenkėjiškus veiksmus, laikoma, kad programoje yra pažeidimas, užuot priskyrus ją užpakalinių durų kenkėjiškų programų kategorijai, ir kūrėjo prašoma ją pataisyti.

Užmaskuota programinė įranga

Programa, kurioje naudojami įvairūs apgaulingi būdai siekiant pateikti naudotojui kitokias, nei nurodyta, arba suklaidintas programos funkcijas. Šios programos yra užmaskuotos kaip teisėtos programos ar žaidimai, kad programų parduotuvėse atrodytų nežalingos. Jose naudojami tokie metodai kaip klaidinimas, dinaminis kodo įkėlimas arba pridengimas siekiant paslėpti kenkėjišką turinį.

Užmaskuota programinė įranga yra panaši į kitų PŽP kategorijų programinę įrangą, ypač Trojos arklių. Pagrindinis skirtumas yra metodai, naudojami kenkėjiškai veiklai užmaskuoti.

Apsimetinėjimas

Neleidžiame teikti programų, kuriose naudotojai klaidinami apsimetant kuo nors kitu (pvz., kitu kūrėju, įmone, subjektu) ar kita programa. Negalima teigti, kad jūsų programa yra susijusi su kitu asmeniu ar jo įgaliota, jei taip nėra. Būkite atsargūs ir nenaudokite programos piktogramų, aprašų, pavadinimų ar elementų programoje, galinčių klaidinti naudotojus dėl programos ryšio su kitu asmeniu ar kita programa.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Kūrėjai, kurie klaidingai nurodo ryšį su kita įmone, kūrėju, subjektu ir (arba) organizacija.

① Pateiktas šios programos kūrėjo pavadinimas nurodo oficialų ryšį su „Google“, bet iš tikrųjų taip nėra.

- Programos, kurių piktogramose ir pavadinimuose klaidingai nurodomas ryšys su kita įmone, kūrėju, subjektu ir (arba) organizacija.

① Programoje naudojamas nacionalinis ženklėjimas ir naudotojams klaidingai nurodomas jos ryšys su vyriausybe.

② Programoje naudojamas nukopijuotas verslo subjekto logotipas, klaidingai nurodant, kad ji yra oficiali įmonės programa.

- Programų pavadinimai ir piktogramos labai panašios į esamų programų ar paslaugų pavadinimus ir piktogramas, todėl naudotojai gali būti klaidinami.

- ① Programos piktogramoje naudojamas populiarios kriptovaliutos svetainės logotipas, nurodant, kad tai yra oficiali svetainė.
 - ② Programos piktogramoje naudojamas nukopijuotas žinomos TV laidos personažas ir pavadinimas, naudotojams klaidingai nurodant, kad ji susijusi su TV laida.
 - Programos, kurios melagingai nurodo, kad yra oficiali žinomo subjekto programa. Neturint reikiamų leidimų ar teisių neleidžiama naudoti pavadinimų, pvz., „Oficiali Justino Bieberio programa“.
 - Programos, pažeidžiančios „Android“ prekės ženklo gaires .
-

Mobiliesiems skirta nepageidaujama programinė įranga

„Google“ tiki, kad jei dėmesį sutelksime į naudotoją, visa kita įvyks savaime. [Programinės įrangos principuose](#) ir [nepageidaujamos programinės įrangos politikoje](#) pateikiame bendrąsias programinės įrangos, teikiančios tinkamas funkcijas naudotojams, rekomendacijas. Ši politika pagrįsta „Google“ nepageidaujamos programinės įrangos politika, kurioje apibrėžiami „Android“ ekosistemos ir „Google Play“ parduotuvės principai. Šiuos principus pažeidžianti programinė įranga yra potencialiai žalinga naudotojui teikiamoms paslaugoms, todėl imsime veiksmų, kad apsaugotume naudotojus nuo jos.

Kaip minėta [nepageidaujamos programinės įrangos politikoje](#), nustatėme, kad dauguma nepageidaujamos programinės įrangos pasižymi bent viena ta pačia pagrindine savybe.

- Tai apgaulingi, vertės pasiūlymų teiginiai, kurių programinė įranga neatitinka.
- Ji bando apgaule priversti naudotojus įdiegti ją arba susieja kelias žymas diegiant kitą programą.
- Ji nepraneša naudotojui apie visas savo pagrindines ir svarbiausias funkcijas.
- Ji paveikia naudotojo sistemą netikėtais būdais.
- Ji renka arba perduoda privačią informaciją be naudotojų žinios.
- Ji renka arba perduoda privačią informaciją saugiai jos neapdorodama (pvz., perduoda per HTTPS).
- Ji susieta su kita programine įranga ir jos egzistavimas neatskleidžiamas.

Mobiliuosiuose įrenginiuose programinė įranga yra programos, dvejetainės programos, sistemos modifikavimo ir pan. formos kodas. Siekdami išvengti programinės įrangos, kenkiančios programinės įrangos ekosistemai ar trikdančios naudotojo patirtį, imsime veiksmų, susijusių su kodu, kuris pažeidžia šiuos principus.

Toliau remiamės nepageidaujamos programinės įrangos politika, kad išplėstume jos taikymą mobiliesiems skirtai programinei įrangai. Kaip ir atsižvelgdami į šią politiką, ir toliau tobulinsime šią nepageidaujamos programinės įrangos mobiliesiems politiką, kad galėtume spręsti naujų tipų piktnaudžiavimą.

Skaidri elgsena ir aiškūs paskelbimai

Visas kodas turi atitikti naudotojui pateiktus pažadus. Programose turėtų būti teikiamos visos nurodytos funkcijos. Programos neturėtų klaidinti naudotojų.

- Programose turi būti aiškiai nurodytos funkcijos ir tikslai.

- Išsamiai ir aiškiai paaiškinkite naudotojui, kokius sistemos pakeitimus atliks programa. Leiskite naudotojams peržiūrėti ir patvirtinti visas svarbias diegimo parinktis ir pakeitimus.
- Programinė įranga neturėtų klaidingai pateikti naudotojo įrenginio būsenos, pvz., teigiant, kad sistema yra kritinės saugos būsenos arba užkrėsta virusais.
- Nevykdykite netinkamos veiklos, skirtos skelbimų srautui ir (arba) konversijų skaičiui padidinti.
- Neleidžiame teikti programų, kuriose naudotojai klaidinami apsimetant kuo nors kitu (pvz., kitu kūrėju, įmone, subjektu) ar kita programa. Negalima teigti, kad jūsų programa yra susijusi su kitu asmeniu ar jo įgaliota, jei taip nėra.

Toliau pateikiama pažeidimų pavyzdžių.

- Apgaulingi skelbimai
- Socialinė inžinerija

Apsaugokite naudotojų duomenis ir privatumą

Aiškiai ir išsamiai nurodykite prieigą prie asmens ir neskelbtinų naudotojų duomenų, jų naudojimą, rinkimą ir bendrinimą. Naudotojų duomenų naudojimas turi atitikti visą atitinkamą naudotojų duomenų politiką (jei taikoma) ir turi būti imamasi visų atsargumo priemonių duomenims apsaugoti.

- Suteikite naudotojams galimybę sutikti su duomenų rinkimu prieš pradėdami rinkti ir siųsti duomenis iš įrenginio, įskaitant duomenis apie trečiųjų šalių paskyras, el. pašto adresus, telefonų numerius, įdiegtas programas, failus, vietovę ir kitus asmens bei neskelbtinus duomenis, kurių rinkimo naudotojas negalėtų numatyti.
- Surinkti asmens ir neskelbtini naudotojų duomenys turėtų būti saugiai apdorojami, įskaitant perdavimą naudojant modernią kriptografiją (pvz., per HTTPS).
- Programinė įranga, įskaitant programas mobiliesiems, į serverius turi perduoti tik asmens ir neskelbtinus naudotojų duomenis, susijusius su programos funkcijomis.
- Neprašykite ir neklaidinkite naudotojų, kad jie išjungtų įrenginio saugos priemones, pvz., „Google Play Protect“. Pavyzdžiui, negalite siūlyti naudotojams papildomų programos funkcijų ar premijų mainais už „Google Play Protect“ išjungimą.

Toliau pateikiama pažeidimų pavyzdžių.

- Duomenų rinkimas (palyginti su [šnipinėjimo programa](#))
- Piktnaudžiavimas ribotais leidimais

Toliau pateikiama naudotojų duomenų politikos pavyzdžių.

- [„Google Play“ naudotojų duomenų politika](#)
- [GPM reikalavimų naudotojų duomenų politika](#)
- [„Google“ API paslaugos naudotojų duomenų politika](#)

Nepakenkite mobiliesiems teikiamoms funkcijoms

Naudotojams teikiamos funkcijos turi būti paprastos, lengvai suprantamos ir aiškos. Naudotojui turi būti pateiktas aiškus vertės pasiūlymas ir neturi būti sutrikdomos reklamuojamos ar pageidaujamos naudotojams teikiamos funkcijos.

- Nerodykite skelbimų, kurie naudotojams pateikiami nenumatytais būdais, pvz., pakenkiant įrenginio funkcijoms ar trikdyti jų veikimą arba pateikiant ne aktyvinamosios programos aplinkoje, jei jų negalima lengvai atsakyti ir gauti tinkamo sutikimo bei priskyrimo.
- Programos neturėtų trukdyti kitoms programoms ar naudoti įrenginį.
- Pašalinimas turėtų būti aiškus (jei taikoma).
- Programinė įranga mobiliesiems neturėtų imituoti raginimų iš įrenginio OS ar kitų programų. Neleiskite įspėjimų naudotojui iš kitų programų ar operacinės sistemos, ypač tų, kurie informuoja naudotoją apie OS pakeitimus.

Toliau pateikiama pažeidimų pavyzdžių.

- Veikimą trikdančios skelbimai
 - Neteisėtos sistemos funkcijų naudojimas ar imitavimas
-

Kenkėjiškos atsisiuntimo programos

Kodas, kuris nėra nepageidaujama programinė įranga, bet jį naudojant atsisiunčiama kita nepageidaujama programinė įranga mobiliesiems (angl. „mobile unwanted software“, „MUwS“).

Kodas gali veikti kaip kenkėjiška atsisiuntimo programa, jei:

- galima pagrįstai manyti, kad jis buvo sukurtas siekiant platinti „MUwS“ ir jį naudojant buvo atsisiųsta „MUwS“ arba jis apima kodą, kurį naudojant galima atsisiųsti ir įdiegti programas; arba
- mažiausiai penki procentai jį naudojant atsisiųstų programų yra „MUwS“, kai minimalus stebimų programų atsisiuntimų slenkstis yra 500 (25 stebimi „MUwS“ atsisiuntimai).

Pagrindinės naršyklės ir failų bendrinimo programos nėra laikomos kenkėjiškomis atsisiuntimo programomis, jei:

- jos neskatina atsisiuntimų naudotojui neatliekant veiksmų ir
 - visi programinės įrangos atsisiuntimai vykdomi gavus naudotojų sutikimą.
-

Apgaulingi skelbimai

Apgaulingi skelbimai griežtai draudžiami. Sąveikos su skelbimais, sugeneruotos siekiant apgauti skelbimų tinklą, kad būtų galima manyti, jog srautas yra iš autentiško naudotojo susidomėjimo, yra apgaulingas skelbimas, o tai yra [netinkamo srauto](#) forma. Apgaulingi skelbimai gali būti kūrėjų, kurie skelbimus diegia neleistiniais būdais, pvz., rodo paslėptus skelbimus, automatiškai spustelėja skelbimus, keičia ar modifikuoja informaciją ir kitaip paskatina ne žmonių veiksmus (vorai, robotai ir pan.) arba žmogaus veiklą, kuria siekiama sukurti netinkamą skelbimų srautą. Netinkamas srautas ir apgaulingi skelbimai kenkia reklamuotojams, kūrėjams ir naudotojams, todėl ilgam laikui prarandamas pasitikėjimas skelbimų mobiliesiems ekosistema.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

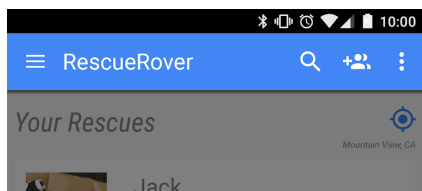
- Programa, kurioje pateikiami naudotojui nematomi skelbimai.
 - Programa, kuri automatiškai generuoja skelbimų paspaudimus be naudotojo ketinimų arba sukuria atitinkamą tinklo srautą, kad apgaulingai priskirtų paspaudimus.
 - Programa, siunčianti netikrus diegimo priskyrimo paspaudimus, kad būtų sumokėta už diegimus, kurie nebuvo iš siuntėjo tinklo.
 - Programa, kurioje iššokantieji skelbimai rodomi, kai naudotojas nenaudoja programos sąsajos.
 - Klaidingas skelbimų vietų pristatymas programoje, pvz., programa, kuri nurodo skelbimų tinklams, kad ji veikia „iOS“ įrenginyje, kai iš tikrųjų yra vykdoma „Android“ įrenginyje; programa, kurioje klaidingai pristatomas paketo, iš kurio gaunama pajamų, pavadinimas.
-

Neteisėtos sistemos funkcijų naudojimas ar imitavimas

Neleidžiame teikti programų ar skelbimų, kuriuose mėgdžiojamos ar trikdomos sistemos funkcijos, pvz., pranešimai ar įspėjimai. Sistemos lygio pranešimus galima naudoti tik svarbiausioms programos funkcijoms, pvz., oro linijų programoje, kuri praneša naudotojams apie specialius pasiūlymus, ar žaidime, kuriame naudotojams rodomos reklamos.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Programos ar skelbimai, teikiami sistemos pranešime ar įspėjime.



① Šioje programoje rodomas sistemos pranešimas naudojamas skelbimui pateikti.

Jei reikia papildomų pavyzdžių, apimančių skelbimus, žr. [skelbimų politiką](#).

Socialinė inžinerija

Neleidžiame teikti programų, kurios apsimeta kita programa, siekiant paskatinti naudotojus atlikti veiksmus, skirtus patikimai pradinei programai.

Pajamų gavimas ir skelbimai

„Google Play“ palaikomos įvairios pajamų gavimo strategijos, naudingos kūrėjams ir naudotojams, įskaitant mokamą platinimą, produktus programoje, prenumeratas ir skelbimais pagrįstus modelius. Siekdami užtikrinti, kad naudotojams teikiamos kuo geresnės paslaugos, reikalaujame laikytis šios politikos.

Mokėjimai

1. Už programų atsisiuntimus iš „Google Play“ apmokestinantys kūrėjai kaip mokėjimo už šias operacijas metodą turi naudoti „Google Play“ atsiskaitymo sistemą.
2. Sistemoje „Play“ platinamose programose, kuriose reikalaujamas ar priimamas mokėjimas už galimybę pasiekti funkcijas ar paslaugas programoje, įskaitant bet kokias programos funkcijas, skaitmeninį turinį ar prekes (bendrai vadinama pirkiniais programoje), reikia naudoti „Google Play“ atsiskaitymo sistemą šioms operacijoms, nebent taikoma trečia, aštunta arba devinta skiltis.

Programų funkcijų ar paslaugų, kurioms reikia naudoti „Google Play“ atsiskaitymo sistemą, pavyzdžiai apima toliau nurodytus pirkinius programoje (bet jais neapsiribojama).

- Elementai (pvz., virtualioji valiuta, papildomos gyvybės, papildomas žaidimo laikas, priedų elementai, personažai ir pseudoportretai).

- Prenumeratos paslaugos (pvz., kūno rengybos, žaidimų, pažinčių, švietimo, muzikos, vaizdo įrašų, paslaugų naujovinių ir kito turinio prenumeratos paslaugos).
- Programos funkcijos ar turinys (pvz., programos versija be skelbimų arba naujos funkcijos, kurios nepasiekiamos versijos be piniginio mokėjimo programoje).
- Programinė įranga ir paslaugos debesyje (pvz., duomenų saugyklos paslaugos, verslo produktyvumo ir finansų tvarkymo programinė įranga).

3. „Google Play“ atsiskaitymo sistemos negalima naudoti toliau nurodytais atvejais.

a. Kai mokėjimas pirmiausia skirtas:

- fizinėms prekėms įsigyti ar nuomoti (pvz., maisto prekėms, drabužiams, namų apyvokos daiktams, elektronikos prekėms);
- fizinėms paslaugoms įsigyti (pvz., transporto, valymo paslaugoms, lėktuvų bilietams, sporto klubo narystei, maisto pristatymo paslaugoms, bilietams į tiesioginius įvykius) arba
- pinigams pervesti apmokant kredito kortelės ar komunalinių paslaugų sąskaitą (pvz., už kabelinę televiziją ir telekomunikacijų paslaugas).

b. Mokėjimai apima mokėjimus tarp naudotojų, internetinius aukcionus ir aukas, kurioms netaikomi mokesčiai.

c. Mokėjimas atliekamas už internetinį lošimą skatinantį turinį ar paslaugas, kaip aprašyta [Lošimo programų](#) skiltyje [Lošimo iš tikrų pinigų, žaidimų ir konkursų politikoje](#).

d. Mokėjimas taikomas bet kuriai produktų kategorijai, kuri pagal „Google“ [mokėjimų centro turinio politiką](#) laikoma nepriimtina.

Pastaba: kai kuriose rinkose teikiame „Google Pay“ programoms, kuriose parduodamos fizinės prekės ir (arba) paslaugos. Jei reikia daugiau informacijos, apsilankykite [„Google Pay“ kūrėjo puslapyje](#).

4. Programose naudotojai negali būti nukreipiami naudoti kitą mokėjimo metodą nei „Google Play“ atsiskaitymo sistema, išskyrus trečioje, aštuntoje ir devintoje skiltyse nurodytas sąlygas. Šis draudimas apima (bet tuo neapsiribojama) naudotojų nukreipimą į kitus mokėjimo metodus naudojant:

- programos įrašą sistemoje „Google Play“;
- su įsigyjamu turiniu susijusias reklamas programoje;
- žiniatinklio rodinius, mygtukus, nuorodas, pranešimus, skelbimus ar kitus raginimus veikti programoje ir
- naudotojo sąsajos programoje srautus, įskaitant paskyros kūrimo ar prisiregistravimo srautus, kurie nukreipia naudotojus iš programos į kitą mokėjimo metodą nei „Google Play“ atsiskaitymo sistema.

5. Virtualioji valiuta programoje turi būti naudojama tik toje programoje, kurioje ji buvo įsigyta pirmą kartą.

6. Kūrėjai turi aiškiai ir tiksliai informuoti naudotojus apie programos ar bet kokių funkcijų programoje ar prenumeratų, kurias siūloma įsigyti, sąlygas ir kainas. Kainodara programoje turi atitikti kainą, pateiktą naudotojams skirtoje „Google Play“ atsiskaitymo sąsajoje. Jei jūsų produkto apraše „Google Play“ nurodomos funkcijos programoje, kurioms taikomas konkretus ar papildomas mokestis, programos įrašė naudotojams turi būti aiškiai nurodyta, kad norint pasiekti tas funkcijas reikės sumokėti.

7. Programose ir žaidimuose, kuriuose teikiami atsitiktinai atrenkamų virtualių elementų gavimo perkant mechanizmai, įskaitant „laimėjimų dėžutes“, bet jomis neapsiribojant, iš anksto ir tinkamu laiku prieš perkant turi būti aiškiai atskleisti šių elementų gavimo šansai.

8. Jei netaikomos trečioje skiltyje nurodytos sąlygos, sistemoje „Play“ platinamų programų, kuriose reikalaujamas ar priimamas mokėjimas iš naudotojų šiose [šalyse / regionuose](#) už galimybę pasiekti pirkinius programoje, kartu su „Google Play“ atsiskaitymo sistema kūrėjai gali teikti naudotojams alternatyvaus atsiskaitymo sistemą, skirtą tokioms operacijoms, sėkmingai užpildę kiekvienos

atitinkamos programos atsiskaitymo deklaracijos formą ir sutikę su papildomomis sąlygomis bei į jas įtrauktais [programų reikalavimais](#).

9. „Google Play“ sistemoje platinamų programų kūrėjai gali nukreipti naudotojus Europos ekonominėje erdvėje (EEE) už programos ribų, įskaitant skaitmeninių funkcijų programose ar paslaugų pasiūlymų reklamavimą. Kūrėjai, nukreipiantys EEE naudotojus už programos ribų, turi sėkmingai užpildyti programos [deklaracijos formą](#) ir sutikti su papildomomis taisyklėmis bei į jas įtrauktais [programos reikalavimais](#).

Pastaba: jei norite peržiūrėti terminus ir dažniausiai užduodamus klausimus apie šią politiką, apsilankykite [pagalbos centre](#).

Skelbimai

Siekdami užtikrinti kokybišką patirtį atsižvelgiame į skelbimo turinį, auditoriją, naudotojų patirtį, elgseną bei saugą ir privatumą. Skelbimus ir susijusius pasiūlymus laikome programos dalimi, todėl jie taip pat turi atitikti visas kitas „Google Play“ politikos nuostatas. Be to, taikome papildomus reikalavimus skelbimams, jei gaunate pajamų iš programos, kuri taikoma pagal vaikus sistemoje „Google Play“.

Daugiau informacijos apie programos reklamos ir parduotuvės įrašo politiką taip pat pateikiama [čia](#), įskaitant informaciją, kaip elgiamės su [apgaulinga reklama](#).

Skelbimo turinys

Skelbimai ir susiję pasiūlymai yra programos dalis ir turi atitikti [apriboto turinio](#) politiką. Jei jūsų programa yra [lošimo](#) programa, taikomi papildomi reikalavimai.

Netinkami skelbimai

Programoje rodomi skelbimai ir su jais susiję pasiūlymai (pvz., skelbime reklamuojamas kitos programos atsisiuntimas) turi atitikti programos [turinio įvertinimą](#), net jei pats turinys atitinka kitas politikos nuostatas.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Pagal programos turinio įvertinimo netinkami skelbimai

- ① Šis skelbimas (skirtas paaugliams) neatitinka programos turinio įvertinimo (skirta visiems)
- ② Šis skelbimas (skirtas suaugusiesiems) neatitinka programos turinio įvertinimo (skirta paaugliams)
- ③ Skelbimo pasiūlymas (kuriame reklamuojamas suaugusiesiems skirtos programos atsisiuntimas) neatitinka žaidimo programos, kurioje skelbimas buvo pateiktas, turinio įvertinimo (skirta visiems)

Šeimai skirtų skelbimų reikalavimai

Jei gaunate pajamų iš programos, kuri taikoma pagal vaikus, sistemoje „Google Play“, programa turi atitikti [šeimoms skirtų skelbimų ir pajamų gavimo politikos reikalavimus](#).

Apgaulingi skelbimai

Skelbimuose neturi būti imituojama bet kurios programos funkcijos naudotojo sąsaja, pvz., operacinės sistemos pranešimai ar įspėjamieji elementai. Naudotojas turi aiškiai suprasti, kuri programa pateikia skelbimą.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Skelbimai, imituojantys programos NS:

① Šioje programoje pateikiama klaustuko piktograma yra skelbimas, nukreipiantis naudotoją į išorinį nukreipimo puslapį.

- Skelbimai, imituojantys sistemos pranešimus:

① ② Anksčiau pateiktuose pavyzdžiuose rodomi skelbimai, imituojantys įvairius sistemos pranešimus.

① Anksčiau pateiktame pavyzdyje rodoma funkcijų skiltis, kuri imituoja kitas funkcijas, bet tik nukreipia naudotoją į skelbimą ar skelbimus.

Veikimą trikdančios skelbimai

Veikimą trikdančios skelbimai – tai skelbimai, kurie naudotojams pateikiami nenumatytais būdais, skatinant netyčinius paspaudimus arba pakenkiant įrenginio funkcijoms ar trikdančią jų veikimą.

Jūsų programa negali priverstinai skatinti naudotojo spustelėti skelbimą ar pateikti asmeninę informaciją reklamavimo tikslais, kad būtų galima naudotis visomis programos funkcijomis. Skelbimai gali būti rodomi tik programoje, kurioje jie teikiami, ir negali trukdyti kitoms programoms, skelbimams ar įrenginio veikimui, įskaitant sistemos ar įrenginio mygtukus ir prievadus. Tai apima perdangas, susijusias funkcijas ir į valdiklius įtrauktus skelbimų rinkinius. Jei jūsų programoje rodomi skelbimai ar kiti skelbimai, kurie trikdo įprastą naudojimą, turi būti suteikta galimybė lengvai jų atsisakyti be nuobaudų.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Visą ekraną užimantys ar įprastą naudojimą trikdančios skelbimai, kai nesuteikiamas aiškus būdas atsisakyti skelbimo:

① Šiame skelbime nėra atsisakymo mygtuko.

- Skelbimai, kuriuose naudotojas verčiamas spustelėti, naudojant klaidingą atsisakymo mygtuką, arba skelbimai, kurie staiga pasirodo programos srityse, kur naudotojas paprastai paliečia norėdamas naudoti kitą funkciją.

① Šiame skelbime naudojamas klaidingas atsisakymo mygtukas.

② Šis skelbimas staiga rodomas srityje, kurią naudotojas įprastai paliečia, norėdamas naudoti funkcijas programoje.

- Skelbimai, rodomi už juos teikiančios programos ribų:

① Naudotojas iš šios programos eina į pagrindinį ekraną ir staiga pagrindiniame ekrane iššoka skelbimas.

- Skelbimai, kuriuos suaktyvina pagrindinio ekrano mygtukas ar kitos funkcijos, konkrečiai skirtos išeiti iš programos:

① Naudotojas bando išeiti iš programos ir įeiti į pagrindinį ekraną, bet tikėtiną srautą pertraukia iššokęs skelbimas.

Geresnė su skelbimais susijusi patirtis

Kūrėjai turi laikytis toliau nurodytų skelbimų gairių, kad užtikrintų aukštos kokybės funkcijas „Google Play“ programų naudotojams. Skelbimai negali būti rodomi naudotojams toliau nurodytais nenumatytais atvejais.

- Neleidžiami viso ekrano režimu rodomi visų formatų (vaizdo įrašo, GIF, statiniai ir kt.) tarpinio puslapio skelbimai, kurie rodomi netikėtai, įprastai naudotojui pasirinkus atlikti kokius nors kitus veiksmus.
- Neleidžiami skelbimai, kurie rodomi žaidžiant, prasidedant lygiui ar turinio segmentui.
- Neleidžiami viso ekrano režimu rodomi vaizdo įrašo tarpinio puslapio skelbimai, kurie rodomi prieš pateikiant programos įkėlimo ekraną (prisistatymo langą).
- Neleidžiami viso ekrano režimu rodomi visų formatų tarpinio puslapio skelbimai, kurie neuždaromi po penkiolikos sekundžių. Pasirenkami viso ekrano režimu rodomi tarpinio puslapio skelbimai arba viso ekrano režimu rodomi tarpinio puslapio skelbimai, kurie netrikdo naudotojų veiksmų (pvz., pateikus rezultatų ekraną žaidimo programoje), gali būti rodomi ilgiau nei penkiolika sekundžių.

Ši politika netaikoma atlyginamiems skelbimams, kuriuos aiškiai pasirenka naudotojai (pvz., skelbimui, kurį kūrėjas aiškiai siūlo naudotojui peržiūrėti, kad būtų atrakinta konkreti žaidimo funkcija ar turinio dalis). Be to, ši politika netaikoma pajamų gavimo ir reklamavimo skelbimams, kurie netrikdo įprasto programos naudojimo ar žaidimo eigos (pvz., vaizdo įrašo turiniui su integruotais skelbimais, ne viso ekrano režimu rodomiems reklamjuostės skelbimams).

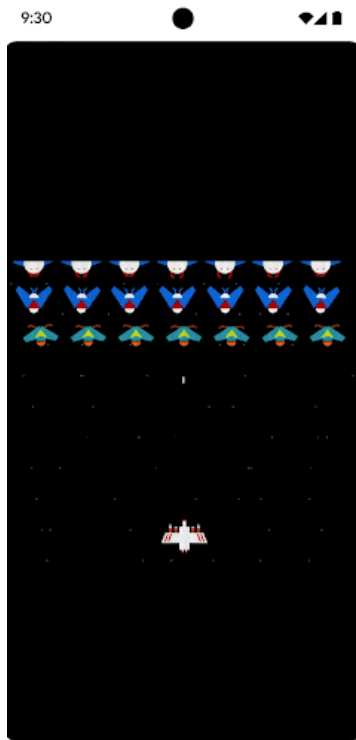
Šios gairės pagrįstos [geresnių skelbimų standartų – programų mobiliems funkcijų](#) gairėmis. Jei reikia daugiau informacijos apie geresnių skelbimų standartus, žr. [Geresnių skelbimų sąjungos](#) informaciją.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Netikėti skelbimai, kurie rodomi žaidžiant žaidimą ar prasidedant turinio segmentui (pvz., naudotojui spustelėjus mygtuką, prieš prasidedant veiksmui, kuris turėtų būti atliekamas spustelėjus mygtuką). Šie skelbimai yra netikėti naudotojams, nes naudotojai tikisi pradėti žaidimą ar sąveikauti su turiniu.

① Netikėtas statinis skelbimas, rodomas žaidžiant, prasidedant lygiui.

- ② Netikėtas vaizdo įrašo skelbimas, rodomas prasidedant turinio segmentui.
- Viso ekrano režimu rodomas skelbimas, kuris pateikiamas žaidžiant ir kurio negalima uždaryti po penkiolikos sekundžių.



- ① Tarpinio puslapio skelbimai, kurie rodomi žaidžiant ir kuriuose naudotojams nepateikiama parinktis praleisti skelbimą per penkiolika sekundžių.

Sukurta skelbimams

Neleidžiame programų, kuriose pakartotinai teikiami tarpinio puslapio skelbimai, siekiant trikdyti naudotojų sąveiką su programa ir neleisti atlikti užduočių programoje.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Programos, kuriose tarpinio puslapio skelbimas pateikiamas iš karto naudotojui atlikus veiksmą (įskaitant paspaudimus, perbraukimus ir pan., bet jais neapsiribojant).

① Pirmajame programos puslapyje yra daug naudotinių mygtukų. Naudotojui spustelėjus **Paleisti programą**, norint naudoti programą, iššoka tarpinio puslapio skelbimas. Uždaręs skelbimą naudotojas grįžta į programą ir spustelėja **Paslauga**, norėdamas pradėti naudoti paslaugą, bet parodomas kitas tarpinio puslapio skelbimas.

② Pirmajame puslapyje naudotojas nukreipiamas spustelėti mygtuką **Leisti**, nes tai vienintelis pasiekiamas mygtukas norint naudoti programą. Naudotojui jį spustelėjus parodomas tarpinio puslapio skelbimas. Uždaręs skelbimą naudotojas spustelėja **Pristatyti**, nes tai vienintelis pateiktas mygtukas, ir iššoka kitas tarpinio puslapio skelbimas.

Pajamų gavimas užrakintu ekranu

Jei užrakintas ekranas nėra išskirtinis programos tikslas, programose gali nebūti teikiami skelbimai ar funkcijos, iš kurių gaunamos pajamos veikiant įrenginyje užrakintu ekranu.

Apgaulingi skelbimai

Apgaulingi skelbimai griežtai draudžiami. Jei reikia daugiau informacijos, žr. [apgaulingų skelbimų politiką](#).

Vietovės duomenų naudojimas skelbimams

Programoms, praplečiančioms tik su leidimu pasiekiamos įrenginio vietovės duomenų naudojimą siekiant teikti skelbimus, taikoma [asmens ir neskelbtinos informacijos](#) politika ir jos taip pat privalo laikytis toliau nurodytų reikalavimų.

- Tik su leidimu pasiekiamos įrenginio vietovės duomenų naudojimas ir rinkimas siekiant reklamuoti turi būti aiškus naudotojui ir dokumentuotas privalomoje programos privatumo politikoje, įskaitant susiejimą su bet kokiomis susijusiomis skelbimų tinklo privatumo politikomis, apibrėžiančiomis vietovės duomenų naudojimą.
- Laikantis [leidimo pasiekti vietovės duomenis](#) reikalavimų, užklauso dėl leidimų pasiekti vietovės duomenis gali būti teikiamos tik siekiant įdiegti dabartines programos funkcijas ar paslaugas ir

negalima teikti leidimo pasiekti įrenginio vietovės duomenis užklausų siekiant vien tik naudoti skelbimus.

„Android“ reklamavimo ID naudojimas

4.0 versijos „Google Play“ paslaugose pateikiami nauji API ir ID, skirti reklamavimo ir analizės teikėjams. Šių ID naudojimo sąlygos nurodytos toliau.

- **Naudojimas.** „Android“ reklamavimo identifikatorių (angl. „Android advertising identifier“, AAID) galima naudoti tik reklamavimo ir naudotojų analizės tikslais. Kaskart pasiekiant ID turi būti patvirtinta nustatymo „Atsisakyti reklamavimo pagal pomėgius“ arba „Atsisakyti skelbimų suasmeninimo“ būseną.
- **Susiejimas su asmens identifikavimo informacija ar kitais identifikatoriais.**
 - Reklamavimo naudojimas: reklamavimo identifikatorius negali būti susietas su nuolatiniais įrenginio identifikatoriais (pvz., SSAID, MAC adresu, IMEI ir kt.) jokiais reklamavimo tikslais. Reklamavimo identifikatorių galima susieti su asmens identifikavimo informacija tik gavus aiškų naudotojo sutikimą.
 - „Analytics“ naudojimas: reklamavimo identifikatoriaus negalima susieti su asmens identifikavimo informacija ar bet koku nuolatinio įrenginio identifikatoriumi (pvz., SSAID, MAC adresu, IMEI ir kt.) jokiais analizės tikslais. Jei reikia papildomos informacijos apie nuolatinius įrenginio identifikatorius, perskaitykite [Naudotojo duomenų politiką](#).
- **Naudotojų pasirinkimo paaiskymas.**
 - Nustačius iš naujo negalima sujungti naujo reklamavimo identifikatoriaus su ankstesniu reklamavimo identifikatoriumi ar duomenimis, gautais iš ankstesnio reklamavimo identifikatoriaus, be aiškaus naudotojo sutikimo.
 - Privalote atsižvelgti į naudotojo nustatymą „Atsisakyti reklamavimo pagal pomėgius“ arba „Atsisakyti skelbimų suasmeninimo“. Jei naudotojas įgalino šį nustatymą, negalite naudoti reklamavimo identifikatoriaus kurdami naudotojų profilius reklamavimo tikslais ar naudotojams taikydami suasmenintą reklamavimą. Leidžiama veikla: kontekstinis reklamavimas, dažnumo ribos nustatymas, konversijų stebėjimas, ataskaitų teikimas ir saugumo trikčių bei apgaulingos veiklos aptikimas.
 - Naujesniuose įrenginiuose identifikatorius bus pašalintas, jei naudotojas ištrins „Android“ reklamavimo identifikatorių. Bandant pasiekti identifikatorių bus pateikta eilutė su nuliais. Įrenginio be reklamavimo identifikatoriaus negalima susieti su duomenimis, susietais su ankstesniu reklamavimo identifikatoriumi arba gautais jį naudojant.
- **Skaidrumas naudotojams.** Informacijos rinkimas ir reklamavimo identifikatoriaus naudojimas bei įsipareigojimas laikytis šių taisyklių turi būti nurodyti naudotojams teisėtame privatumo pranešime. Jei norite sužinoti daugiau apie mūsų privatumo standartus, žr. [naudotojų duomenų politiką](#).
- **Naudojimo sąlygų laikymasis.** Reklamavimo identifikatorių galima naudoti tik laikantis „Google Play“ kūrėjų programos politikos nuostatų. Jų taip pat privalo laikytis bet kokia šalis, su kuria bendrinate identifikatorių vykdydami verslą. Visose į sistemą „Google Play“ įkeltose ar joje paskelbtose programose reklamavimo tikslais vietoj visų kitų įrenginio identifikatorių turi būti naudojamas reklamavimo ID (kai jis pasiekiamas įrenginyje).

Jei reikia daugiau informacijos, žr. [naudotojų duomenų politiką](#).

Prenumeratos

Jūs, kaip kūrėjas, negalite klaidinti naudotojų dėl jokių prenumeratos paslaugų ar turinio, siūlomų programoje. Svarbu aiškiai išdėstyti informaciją programoje rodomose reklamose ar prisistatymo languose. Neleidžiame programų, kuriose naudotojams teikiamos apgaulingos ar manipuliatyvios pirkimo funkcijos (įskaitant pirkimą programoje ar prenumeratas).

Turite aiškiai išdėstyti savo pasiūlymą. Pavyzdžiui, turite aiškiai nurodyti pasiūlymo sąlygas, prenumeratos kainą, atsiskaitymo ciklo dažnį ir ar norint naudotis programa būtina prenumerata.

Naudotojai neturėtų atlikti jokių papildomų veiksmų, kad galėtų peržiūrėti informaciją.

Prenumeratos turi teikti nuolatinę ar pasikartojančią vertę naudotojams per visą prenumeratos laikotarpį ir negali būti naudojamos siekiant siūlyti naudotojams vienkartinės privilegijas (pavyzdžiui, SKU, kurie suteikia vienkartinius kreditus ir (arba) valiutą programoje arba vienkartinės pagalbinės priemonės žaidime). Jūsų prenumeratoje gali būti siūlomos skatinamosios ar reklaminės premijos, tačiau jos turi papildyti nuolatinę ar pasikartojančią vertę, teikiamą per visą prenumeratos laikotarpį. Produktai, kurie nuolatinės ar pasikartojančios vertės nekuria, turi būti naudojami kaip [produktai programoje](#), o ne kaip [prenumeratos produktai](#).

Negalite maskuoti ar neteisingai apibūdinti vienkartinės naudos naudotojams kaip prenumeratos. Tai apima prenumeratos keitimą (pvz., atšaukimą, teikimo nutraukimą arba pasikartojančios vertės sumažinimą) naudotojui įsigijus prenumeratą, paverčiant ją vienkartinį pasiūlymą.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Mėnesinės prenumeratos, kai naudotojai neinformuojami, kad prenumerata bus automatiškai atnaujinama ir už ją reikės mokėti kas mėnesį.
- Metinės prenumeratos, kurių kainos nurodomos akcentuojant mėnesinius mokesčius.
- Prenumeratos kaina ir sąlygos nevysiškai lokalizuotos.
- Programoje rodomos reklamos, kuriose aiškiai nenurodoma, kad naudotojas gali pasiekti turinį be prenumeratos (kai yra tokia galimybė).
- SKU pavadinimai, kurie aiškiai neapibūdina prenumeratos pobūdžio, pvz., nurodyta „Bandomasis laikotarpis be mokesčio“ arba „Išbandykite „Premium“ narystę – trys dienos be mokesčio“, nors prenumeratai automatiškai taikomas pasikartojantis mokestis.
- Keli pirkimo sekos ekranai, dėl kurių naudotojai gali atsitiktinai spustelėti prenumeravimo mygtuką.
- Nuolatinės ar pasikartojančios vertės neturinčios programos, pvz., kuriose pirmąjį mėnesį siūloma 1 000 brangakmenių, tolesniais prenumeratos mėnesiais sumažinant iki vieno brangakmenio.
- Reikalavimas, kad naudotojas užsiregistruotų gauti automatiškai pratęsiamą prenumeratą, kad būtų suteikta vienkartinė premija, ir naudotojo prenumeratos atšaukimas be jo prašymo jam įsigijus prenumeratą.

Pirmas pavyzdys.

- ① Atsisakymo mygtukas nėra aiškiai matomas ir naudotojai gali nesuprasti, kad galima naudotis funkcija, nesutikus su prenumeratos pasiūlymu.
- ② Pasiūlymas teikiamas nurodant tik vieno mėnesio kainą ir naudotojai gali nesuprasti, kad užsiprenumeravę bus apmokestinti suma už šešis mėnesius.
- ③ Pasiūlyme nurodoma tik pradinė kaina ir naudotojai gali nesuprasti, kad bus automatiškai apmokestinti pasibaigus pradiniam laikotarpiui.
- ④ Pasiūlymas turi būti lokalizuotas ta pačia kalba kaip taisyklės ir nuostatos, kad naudotojai galėtų suprasti jį visą.

Antras pavyzdys.

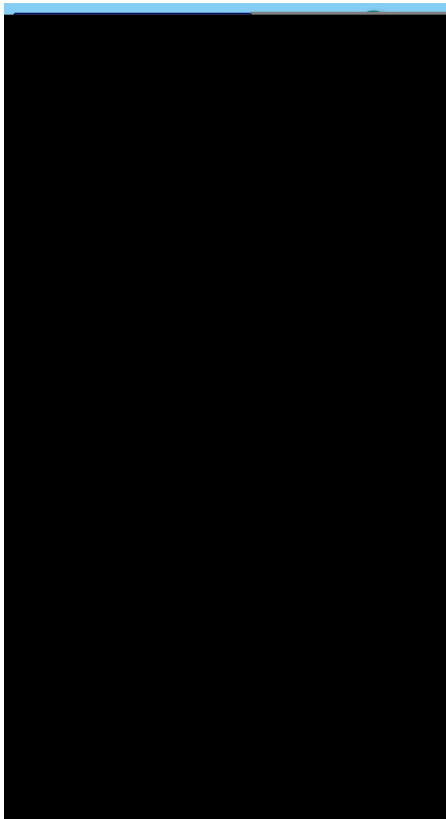
- ① Pasikartojantys paspaudimai toje pačioje mygtuko srityje, dėl kurių naudotojas atsitiktinai spustelėja galutinį tolesnio naudojimo užsakant prenumeratą mygtuką.
- ② Sudėtinga suprasti, kokia suma naudotojai bus apmokestinti pasibaigus bandomajam laikotarpiui, todėl naudotojai gali manyti, kad planui mokėtis netaikomas.

Nemokami bandomieji laikotarpiai ir pradiniai pasiūlymai

Prieš naudotojui užsiregistruojant naudoti jūsų prenumeratą: turite aiškiai ir tiksliai apibūdinti pasiūlymo sąlygas, įskaitant trukmę, kainą ir pasiekiamo turinio ar paslaugų aprašą. Būtinai informuokite naudotojus apie tai, kaip ir kada nemokamas bandomasis laikotarpis taps mokama prenumerata, kiek ji kainuos ir kad naudotojas gali ją atšaukti, jei nenori naudoti mokamos prenumeratos.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Pasiūlymai, kuriuose aiškiai nenurodyta, kiek laiko truks nemokamas bandomasis laikotarpis ar bus siūloma pradinė kaina.
- Pasiūlymai, kuriuose aiškiai nenurodyta, kad pasibaigus pasiūlymo laikotarpiui naudotojas bus automatiškai užregistruotas naudoti mokamą prenumeratą.
- Pasiūlymai, kuriuose aiškiai nenurodyta, kad naudotojas gali pasiekti turinį be bandomojo laikotarpio (kai yra tokia galimybė).
- Pasiūlymo kaina ir sąlygos nevysiškai lokalizuotos.



- ① Atsisakymo mygtukas nėra aiškiai matomas ir naudotojai gali nesuprasti, kad galima pasiekti funkcijas neprisiregistravus nemokamam bandomajam laikotarpiui.
- ② Pasiūlyme akcentuojamas nemokamas bandomasis laikotarpis ir naudotojai gali nesuprasti, kad bus automatiškai apmokestinti pasibaigus bandomajam laikotarpiui.
- ③ Pasiūlyme nenurodomas bandomasis laikotarpis ir naudotojai nežino, kiek laiko galės nemokamai pasiekti prenumeratos turinį.
- ④ Pasiūlymas turi būti lokalizuotas ta pačia kalba kaip taisyklės ir nuostatos, kad naudotojai galėtų suprasti jį visą.

Prenumeratų tvarkymas, atšaukimas ir lėšų grąžinimas

Jei parduodate prenumeratas programoje (-ose), turite užtikrinti, kad programoje (-ose) aiškiai paskelbta, kaip naudotojas gali tvarkyti ar atšaukti savo prenumeratą. Be to, programoje turi būti leidžiama lengvai atšaukti prenumeratą internetu. Programos paskyros nustatymuose (ar atitinkamame puslapyje) šį reikalavimą galite įvykdyti įtraukdami:

- nuorodą į „Google Play“ prenumeratų centrą (jei programoje naudojama „Google Play“ atsiskaitymo sistema) ir (arba)
- tiesioginę prieigą prie atšaukimo proceso.

Pagal mūsų bendrąją politiką, jei naudotojas atšaukia prenumeratą, įsigytą naudojant „Google Play“ atsiskaitymo sistemą, tam naudotojui nebus grąžintos lėšos už dabartinį atsiskaitymo laikotarpį, bet jis ir toliau gaus prenumeratos turinį iki dabartinio atsiskaitymo laikotarpio pabaigos, neatsižvelgiant į atšaukimo datą. Prenumeratos atšaukimas įsigalioja pasibaigus dabartiniam atsiskaitymo laikotarpiui.

Jūs (kaip turinio ar prieigos teisės teikėjas) galite tiesiogiai su naudotojais nustatyti lankstesnę lėšų grąžinimo politiką. Privalote pranešti naudotojams apie bet kokius prenumeratos, atšaukimo ir lėšų grąžinimo politikos pakeitimus ir užtikrinti, kad politikos nuostatos atitinka taikomą įstatymą.

Jei programoje teikiate skelbimų ir į jos tikslinę auditoriją įtraukiami tik vaikai, kaip aprašyta [šeimos politikoje](#) , turite naudoti tik skelbimų SDK, kurie savarankiškai sertifikuoti kaip atitinkantys „Google Play“ politikos nuostatas, įskaitant toliau nurodytus savarankiškai sertifikuotų skelbimų SDK šeimoms reikalavimus.

Jei į programos tikslinę auditoriją įtraukiami vaikai ir vyresni naudotojai, turite užtikrinti, kad vaikams rodomi skelbimai teikiami tik iš vienos iš šių savarankiškai sertifikuotų skelbimų SDK versijų (pvz., naudodami amžiaus filtro priemones).

Atkreipkite dėmesį, kad privalote užtikrinti, jog visos SDK versijos, kurias diegiate savo programoje, įskaitant savarankiškai sertifikuotų skelbimų SDK versijas, atitiktų visas taikomas taisykles, vietas įstatymus ir reglamentus. „Google“ nesuteikia jokių pareiškimų ar garantijų dėl informacijos, kurią skelbimų SDK teikia vykdydami savarankiško sertifikavimo procesą, tikslumo.

Šeimoms skirtus savarankiškai sertifikuotus skelbimų SDK būtina naudoti, tik jei naudojate skelbimų SDK teikdami skelbimus vaikams. Toliau nurodyti elementai leidžiami be skelbimų SDK „Google Play“ savarankiško sertifikavimo, tačiau vis tiek turite užtikrinti, kad skelbimų turinys ir duomenų rinkimo praktika atitinka „Google Play“ [naudotojų duomenų politikos](#) ir [šeimos politikos](#) reikalavimus.

- Vidinis reklamavimas, kai naudojate SDK savo programų ar kitos jums priklausančios medijos ir prekių reklamavimui įvairiose medijose tvarkyti.
- Tiesioginiai pasiūlymai su reklamuotojais, kai naudojate SDK skelbimų vietoms tvarkyti.

Savarankiškai sertifikuotų skelbimų SDK šeimoms reikalavimai

- Apibrėžkite nepriimtina skelbimo turinį bei veiksmus ir nurodykite, kad jie draudžiami, skelbimų SDK taisyklėse ar politikoje. Apibrėžtys turi atitikti „Google Play“ kūrėjų programos politiką.
- Sukurkite skelbimų failų vertinimo pagal konkretaus amžiaus grupės metodą. Konkretaus amžiaus grupės turi apimti bent grupes „Visiems“ ir „Suaugusiesiems“. Vertinimo metodai turi atitikti metodus, kuriuos „Google“ teikia SDK, kai jie užpildo toliau pateiktą dalyvavimo formą.
- Leiskite leidėjams (pateikus užklausą ar naudojant programą) teikti užklausas dėl skelbimų teikimo vaikams skirtame turinyje. Toks turinys turi atitikti galiojančius įstatymus ir nuostatus, pvz., [JAV vaikų privatumo ir apsaugos internete aktą \(angl. „Children's Online Privacy and Protection Act“, COPPA\)](#) ir [ES bendrąjį duomenų apsaugos reglamentą \(BDAR\)](#) . „Google Play“ reikalauja skelbimų SDK išjungti suasmenintus skelbimus, reklamavimą pagal pomėgius ir pakartotinę rinkodarą kaip vaikams skirtą turinio dalį.
- Leiskite leidėjams pasirinkti skelbimų formatus, atitinkančius „Google Play“ [šeimoms skirtų skelbimų ir pajamų gavimo politiką](#) ir [mokytojų patvirtintos programos](#) reikalavimus.
- Užtikrinkite, kad skelbimų failai yra peržiūrimi ir kainų siūlytojams taikomi privatumo rodikliai, kai naudojamas kainų siūlymas realiuoju laiku, siekiant teikti skelbimus vaikams.
- Pateikite „Google“ pakankamai informacijos, pvz., pateikdami bandomąją programą ir informaciją, nurodytą toliau pateiktoje [susidomėjimo formoje](#) , kad būtų galima patvirtinti, jog skelbimų SDK atitinka politiką pagal visus savarankiško sertifikavimo reikalavimus, ir laiku atsakykite į bet kokias vėliau pateiktas informacijos užklausas, pvz., pateikdami naujų versijų leidimus, kad būtų galima patvirtinti skelbimų SDK versijos atitikimą pagal visus savarankiško sertifikavimo reikalavimus.
- [Savarankiškai sertifikuokite](#) , kad visi naujų versijų leidimai atitinka naujausią „Google Play“ kūrėjų programos politiką, įskaitant šeimos politikos reikalavimus.

Pastaba: savarankiškai sertifikuoti skelbimų SDK šeimoms turi palaikyti skelbimų teikimą, atitinkantį visus su vaikais susijusius įstatymus ir reglamentus, kurie gali būti taikomi jų leidėjams.

Daugiau informacijos apie vandens ženklų naudojimą reklaminiuose skelbimo failuose ir bandomąją programą rasite [čia](#) .

Toliau pateikiami teikimo platformoms taikomi tarpininkavimo teikiant skelbimus vaikams reikalavimai.

- Turi būti naudojami tik savarankiškai sertifikuoti skelbimų SDK šeimoms arba taikomos apsaugos priemonės, kuriomis būtų užtikrinta, kad visi iš tarpininkavimo tinklų teikiami skelbimai atitinka šiuos

reikalavimus.

- Perduokite informaciją, reikalingą tarpininkavimo platformoms, norint nurodyti skelbimo turinio įvertinimą ir bet kokią taikomą vaikams skirtą turinį.

Čia kūrėjai gali peržiūrėti savarankiškai sertifikuotų skelbimų SDK šeimoms sąrašą ir patikrinti, kurios konkrečios šių skelbimų SDK versijos yra savarankiškai sertifikuotos naudoti šeimoms skirtose programose.

Be to, kūrėjai gali bendrinti šią [susidomėjimo formą](#) su skelbimų SDK, kurie nori būti savarankiškai sertifikuoti.

Parduotuvės įrašas ir reklama

Programos reklama ir matomumas turi didelės įtakos parduotuvės kokybei. Venkite parduotuvių įrašų, kuriuose yra šlamšto, žemos kokybės reklamų ir pastangų dirbtinai padidinti programos matomumą sistemoje „Google Play“.

Programos reklama

Neleidžiame teikti programų, tiesiogiai ar netiesiogiai susijusių su reklamos strategijomis (pvz., skelbimais), kurios bando apgauti naudotojus ar kūrėjų ekosistemą arba jiems pakenkti. Reklamos strategijos laikomos apgaulingomis arba kenksmingomis, jei jų elgsena ar turinys pažeidžia mūsų Kūrėjų programos politiką.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Svetainėse, programose ar kitose nuosavybėse naudojami [apgaulingi](#) skelbimai, įskaitant pranešimus, kurie panašūs į sistemos pranešimus ir įspėjimus.
- Naudojami [seksualinio pobūdžio](#) skelbimai, nukreipiantys naudotojus į programos „Google Play“ įrašą, kad naudotojai atsisiųstų programą.
- Reklamos ar diegimo taktika, kuri peradresuoja naudotojus į „Google Play“ ar atsisiunčia programas naudotojui neatlikus veiksmų.
- Nepageidaujama reklama naudojant SMS paslaugas.
- Tekstas arba vaizdas programos pavadinime, piktogramoje ar kūrėjo varde, nurodantis parduotuvės našumą arba įvertinimą, kainą ar reklaminę informaciją arba ryšius su esamomis „Google Play“ programomis.

Jūsų pareiga užtikrinti, kad šios politikos būtų laikomasi bet kokiuose skelbimų tinkluose, filialuose ar su programa susietuose skelbimuose.

Metaduomenys

Naudotojai pasikliauja programų aprašais, norėdami suprasti programų funkcijas ir paskirtį. Neleidžiame programų, kuriose teikiami klaidinantys, netinkamai suformatuoti, neaprašomieji, nesusiję, pertekliniai ar netinkami metaduomenys, įskaitant (bet tuo neapsiribojant) programos aprašą, kūrėjo vardą, pavadinimą, piktogramą, ekrano kopijas ir reklaminius vaizdus. Kūrėjai turi pateikti aiškų ir tinkamai parašytą programos aprašą. Be to, programos apraše neleidžiame teikti nepriskirtų ar anoniminių naudotojų atsiliepimų.

Programos pavadinimas, piktograma ir kūrėjo vardas yra ypač naudingi naudotojams, norintiems rasti jūsų programą ir sužinoti apie ją. Nenaudokite jaustukų ar pasikartojančių specialiųjų ženklų tuose metaduomenų elementuose. Venkite TIK DIDŽIŲJŲ RAIDŽIŲ, jei tai nėra prekės ženklo pavadinimo dalis. Klaidinantys simboliai programų piktogramose neleidžiami, pvz.: naujo pranešimo taško indikatorius, kai nėra jokių naujų pranešimų, ir atsisiuntimo / įdiegimo simboliai, kai programa nėra susijusi su turinio atsisiuntimu. Programos pavadinimą gali sudaryti ne daugiau kaip trisdešimt simbolių. Nenaudokite teksto ar vaizdo programos pavadinime, piktogramoje ar kūrėjo varde, nurodančio parduotuvės

našumą arba įvertinimą, kainą ar reklaminę informaciją arba ryšius su esamomis „Google Play“ programomis.

Be čia nurodytų reikalavimų, konkrečioje „Google Play“ kūrėjų politikoje gali būti reikalaujama pateikti papildomos metaduomenų informacijos.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- ① Nepriskirtų ar anoniminių naudotojų atsiliepimai
- ② Programų ar prekių ženklų duomenų palyginimas
- ③ Žodžių blokai ir vertikalūs / horizontalūs žodžių sąrašai

- ① VISOS DIDŽIOSIOS RAIDĖS, jei tai nėra prekės ženklo pavadinimo dalis
- ② Specialiųjų ženklų, kurie nėra susiję su programa, sekos
- ③ Jaustukų (įskaitant japoniškus jaustukus) ir specialiųjų ženklų naudojimas
- ④ Klaidinantys simboliai
- ⑤ Klaidinantis tekstas

- Tekstas ar vaizdai, nurodantys parduotuvės veiklos efektyvumą ar reitingą, pvz., „Metų programa“ „Nr. 1“, „Geriausia 20XX m. „Play“ programa“, „Populiari programa“, apdovanojimų piktogramos ir pan.

- Tekstas ar vaizdai, nurodantys kainą ir reklaminę informaciją, pvz., „10 % nuolaida“, „50 dol. grąžinimas“, „nemokamai tik tam tikrą laikotarpį“ ir pan.

- Tekstas ar vaizdai, nurodantys „Google Play“ programas, pvz., „Redakatoriaus pasirinkimas“, „Naujiena“ ir pan.

Toliau pateikiami keli jūsų įrašė esančio netinkamo teksto, vaizdų arba vaizdo įrašų pavyzdžiai.

- Vaizdai arba vaizdo įrašai su seksualinio pobūdžio turiniu. Venkite seksualinio pobūdžio vaizdų, kuriuose rodomos krūtys, sėdmenys, genitalijos ar kitos seksualinės kūno dalys arba turinys (ilustruotas ar tikras).
- Programos parduotuvės įrašė vartojama nešvanki, vulgari ar kita kalba, netinkama bendrajai auditorijai.
- Aiškiai programos piktogramose, reklaminiuose vaizduose arba vaizdo įrašuose matomas grafinis smurtas.

- Neteisėto vaistų naudojimo vaizdai. Net EDSA (mokomojo, dokumentinio, mokslinio ar meninio) pobūdžio turinys parduotuvės įrašė turi būti tinkamas visoms auditorijoms.

Toliau pateikti keli geriausios praktikos pavyzdžiai.

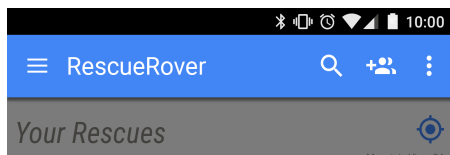
- Pabrėžkite geriausias savo programos savybes. Pasidalykite įdomiais faktais apie savo programą ir padėkite naudotojams suprasti, kuo jūsų programa ypatinga.
- Įsitinkinkite, kad programos pavadinimas ir aprašas tiksliai aprašo jos funkcijas.
- Nenaudokite nesusijusių raktinių žodžių ar nuorodų.
- Programos aprašas turi būti glaustas ir paprastas. Trumpesni aprašai užtikrina geresnę naudotojo patirtį, ypač naudojantis įrenginiais su mažais ekranais. Per ilgą, per daug išsamų, netinkamą formatavimo arba pasikartojantį aprašą gali pažeisti šią politiką.
- Atminkite, kad įrašas turi būti tinkamas bendrajai auditorijai. Įrašė venkite netinkamo teksto, vaizdų ar vaizdo įrašų ir laikykitės anksčiau nurodytų gairių.

Naudotojų įvertinimai, atsiliepimai ir įdiegimai

Kūrėjai neturėtų bandyti manipuliuoti „Google Play“ esančių programų paskirties vietomis. Tai apima produkto įvertinimų, atsiliepimų arba diegimų skaičiaus didinimą neteisėtomis priemonėmis, pvz., apgavikiškais ar skatinamais diegimais, atsiliepimais ir įvertinimais, arba naudotojų skatinimą įdiegti kitas programas kaip pagrindinę programos funkciją (bet tuo neapsiribojama).

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Prašymas naudotojų įvertinti jūsų programą skatinant.



① Šiame pranešime naudotojams siūloma nuolaida mainais už gerą įvertinimą.

- Pakartotinis įvertinimų pateikimas apsimesant naudotojais, siekiant paveikti programos paskirties vietą sistemoje „Google Play“.

- Atsiliepimų su netinkamu turiniu, įskaitant susijusius produktus, kuponus, žaidimų kodus, el. pašto adresus ar nuorodas į svetaines ar kitas programas, pateikimas ar naudotojų skatinimas pateikti tokį turinį.

② Šiame atsiliepime naudotojai skatinami reklamuoti programą „RescueRove“ ir jiems teikiamas kupono pasiūlymas.

Įvertinimai ir atsiliepimai padeda nustatyti programos kokybę. Naudotojams svarbu, kad jie būtų autentiški ir aktualūs. Toliau pateikiama geriausia atsakymo į naudotojų atsiliepimus praktika.

- Sutelkite dėmesį į naudotojo komentare nurodytas problemas ir neprašykite geresnio įvertinimo.
- Įtraukite nuorodą į naudingus išteklius, pvz., palaikymo adresą arba DUK puslapį.

Turinio įvertinimai

Turinio įvertinimus sistemoje „Google Play“ teikia [Tarptautinė amžiaus įvertinimo koalicija \(angl. „International Age Rating Coalition“, IARC\)](#). Jie skirti padėti kūrėjams nurodyti naudotojams turinio įvertinimus pagal vietovę. Regioninės IARC institucijos laikosi gairių, pagal kurias nustatoma programos turinio amžiaus grupė. Neleidžiame teikti programų be turinio įvertinimo sistemoje „Google Play“.

Kaip naudojami turinio įvertinimai

Turinio įvertinimai informuoja klientus, ypač tėvus, apie potencialiai nepageidaujamą programos turinį. Be to, pagal juos galima filtruoti arba blokuoti turinį, kai kuriose teritorijose arba neleisti jo pasiekti konkrečioms naudotojams, kai to reikalaujama pagal įstatymus, ir nustatyti, ar programa gali dalyvauti specialiose kūrėjams skirtose programose.

Kaip priskiriami turinio įvertinimai

Norėdami gauti turinio įvertinimą, turite užpildyti [„Play Console“ įvertinimo anketą](#), kurioje klausiama apie jūsų programų turinio pobūdį. Kelios įvertinimo institucijos priskirs įvertinimą jūsų programos

turiniui pagal anketos atsakymus. Klaidinančiai pristačius programos turinį, ji gali būti pašalinta arba laikinai sustabdyta, todėl būtina tiksliai atsakyti į turinio įvertinimo anketos klausimus.

Kad jūsų programa nebūtų nurodyta kaip „Neįvertinta“, turinio įvertinimo anketą turite pildyti kaskart pateikę naują programą per „Play Console“ ir užpildyti kiekvienos esamos programos, kuri yra aktyvi sistemoje „Google Play“, anketas. Programos, kurių turinys neįvertintas, bus pašalintos iš „Play“ parduotuvės.

Jei pakeitėte programos turinį arba funkcijas ir tai gali turėti įtakos anketos atsakymams, turite pateikti naują turinio įvertinimo anketą per „Play Console“.

Apilankykite [pagalbos centre](#), kur rasite daugiau informacijos apie skirtingas [įvertinimo institucijas](#) ir sužinosite, kaip užpildyti turinio įvertinimo anketą.

Apeliacijos dėl įvertinimų

Jei nesutinkate su jūsų programai priskirtu įvertinimu, galite pateikti apeliaciją tiesiogiai IARC įvertinimo institucijai naudodami sertifikato el. laiške pateiktą nuorodą.

Naujienos

Naujienų programa – tai programa, kuri:

- deklaruojama kaip naujienų programa sistemoje „Google Play Console“ arba
- priskiriama naujienų ir žurnalų kategorijai „Google Play“ parduotuvėje ir kurios pavadinime, piktogramoje, kūrėjo varde ar apraše nurodoma, kad tai yra naujienų programa.

Toliau pateikiama naujienų ir žurnalų kategorijai priskiriamų programų, kurios atitinka naujienų programų reikalavimus, pavyzdžių.

- Programos, kurios savo aprašuose apibrėžiamos kaip naujienų programos, įskaitant (bet tuo neapsiribojant):
 - paskiausias naujienas;
 - laikraščius;
 - karščiausias naujienas;
 - vietines naujienas;
 - dienos naujienas;
- programas, kurių pavadinime, piktogramoje ar kūrėjo varde yra žodis „naujienos“.

Tačiau, jei programose yra pagrindinių naudotojų sukurto turinio (pvz., socialinės medijos programose), jos negali būti apibrėžiamos kaip naujienų programos ir nėra laikomos naujienų programomis.

Naujienų programose, kuriose naudotojas turi įsigyti narystę, prieš įsigyjant turi būti pateikiama naudotojams skirta turinio programoje peržiūra.

Naujienų programose būtina:

- pateikti programos ir naujienų straipsnių šaltinių nuosavybės teisės informaciją, įskaitant (bet tuo neapsiribojant) kiekvieno straipsnio pradinį leidėją ar autorių. Tais atvejais, kai nėra įprasta pateikti individualių straipsnių autorių, naujienų programa turi būti pradinis straipsnių leidėjas. Turėkite omenyje, kad nuorodų į socialinės medijos paskyras nepakanka autorių ar leidėjų informacijai nurodyti;
- nurodyti paskirtą svetainę ar puslapį programoje, kuris aiškiai pažymėtas, kad jame yra kontaktinės informacijos, kurį lengva rasti (pvz., yra nuoroda pagrindinio puslapio apačioje arba svetainės naršymo juostoje) ir kuriame pateikiama galiojanti naujienų leidėjo kontaktinė informacija, įskaitant kontaktinį el. pašto adresą arba telefono numerį. Turėkite omenyje, kad nuorodų į socialinės medijos paskyras nepakanka leidėjų kontaktinei informacijai nurodyti.

Naujienų programose negali būti:

- esminių rašybos ir (arba) gramatikos klaidų;
- vien tik statinio turinio (pvz., daugiau nei trijų mėnesių senumo turinio); ir
- nurodytas pagrindinis tikslas – filialų rinkodara arba pajamos iš skelbimų.

Turėkite omenyje, kad naujienų programose gali būti naudojami skelbimai ir kitų formų rinkodara, siekiant gauti pajamų, kol programos pagrindinė paskirtis nėra parduoti produktus bei paslaugas arba generuoti pajamas iš reklamavimo.

Naujienų programos, kaupiančios turinį iš skirtingų leidimo šaltinių, turi aiškiai nurodyti programos turinio paskelbimo šaltinį ir kiekvienas iš jų turi atitikti naujienų politikos reikalavimus.

[Peržiūrėkite šį straipsnį](#) apie tai, kaip geriausiai pateikti būtiną informaciją.

Šlamštas, funkcijos ir naudotojo patirtis

Programos turėtų teikti bent pagrindines funkcijas ir turinį, kad įtrauktų naudotojus. Užstringančios, netinkamas funkcijas naudotojams teikiančios arba naudotojams ar sistemoje „Google Play“ šlamštą teikiančios programos nėra tinkamos įtraukti į programų katalogą.

Šlamštas

Neleidžiame teikti programų, kurios naudotojams ar „Google Play“ siunčia šlamštą, pvz., programų, kurios naudotojams siunčia nepageidaujamus pranešimus, arba pasikartojančių ir žemos kokybės programų.

Pranešimų šlamštas

Neleidžiame teikti programų, kurios siunčia SMS, el. laiškus ar kitus pranešimus naudotojo vardu, nesuteikdamos naudotojui galimybės patvirtinti turinio ir numatytų gavėjų.

Toliau pateiktas dažnai pasitaikančio pažeidimo pavyzdys.

- Kai naudotojas spustelėja mygtuką „Bendrinti“, programa siunčia pranešimus naudotojo vardu, nesuteikdama galimybės patvirtinti turinio ir numatytų gavėjų:

Žiniatinklio rodiniai ir filialų turinio šlamštas

Neleidžiame teikti programų, kurių pirminis tikslas yra pritraukti filialų srauto į svetainę ar teikti svetainės žiniatinklio rodinį be svetainės savininko ar administratoriaus leidimo.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Svetainė, kurios pirminis tikslas yra į svetainę pritraukti persiuntimo srauto siekiant gauti kredito už naudotojų prisiregistravimus ar pirkinius toje svetainėje.
- Programos, kurių pirminis tikslas yra pateikti svetainės žiniatinklio rodinį be leidimo.

① Ši programa vadinasi „Ted’s Shopping Deals“ ir joje tiesiog pateikiamas „Google“ apsipirkimo žiniatinklio rodinys.

Pasikartojantis turinys

Neleidžiame teikti programų, kuriose teikiamos tik tos pačios funkcijos, kurios jau buvo teikiamos kitose „Google Play“ programose. Programos turėtų suteikti naudotojams naudos, sukurdamos unikalų turinį ar paslaugas.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Turinio kopijavimas iš kitų programų nepridedant jokio originalaus turinio ar vertės.
- Kelių programų su itin panašiu turiniu ir naudotojų funkcijomis kūrimas. Jei šiose programose turinio nedaug, kūrėjai turėtų apsvarstyti galimybę sukurti vieną programą, kurioje būtų sujungiamas visas šis turinys.

Funkcijos, turinys ir naudotojo patirtis

Programose turėtų būti teikiamos stabilios, interaktyvios ir įtraukiančios funkcijos naudotojams. Sistemoje „Google Play“ neleidžiamos programos, kurios užstringa, neteikia bent pagrindinių funkcijų, kad jas būtų galima naudoti kaip programas mobiliesiems, neturi įtraukiančio turinio ar teikia netinkamas bei neįtraukiančias funkcijas naudotojams.

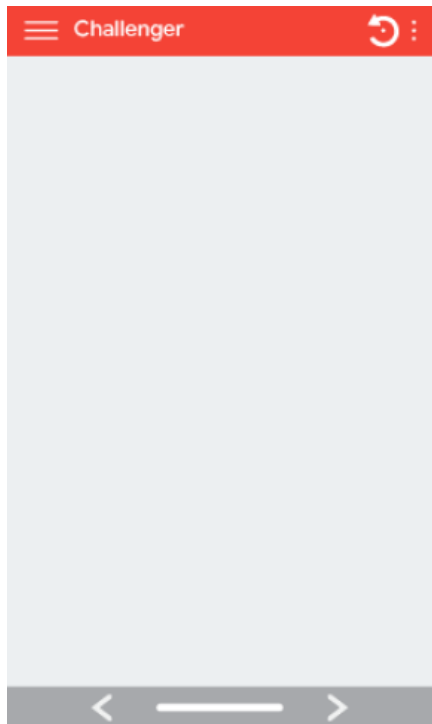
Ribotos funkcijos ir turinys

Neleidžiame programų, kuriose yra tik ribotų funkcijų ir turinio.

Toliau pateiktas dažnai pasitaikančio pažeidimo pavyzdys.

- Programos, kurios yra statinės be konkrečių programų funkcijų, pavyzdžiui, tik teksto ar PDF failų programos
- Programos, kuriose yra labai mažai turinio ir nėra įtraukiančių funkcijų naudotojams, pvz., vieno ekrano fono programos

- Programos, kurios skirtos neatlikti jokių veiksmų ar neturi jokių funkcijų



Sugedusios funkcijos

Neleidžiame užstringančių, priverstinai užsidarančių ar kitaip netinkamai veikiančių programų.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Programos, kurios **neįdiegiamos**
-

Programos, kurios įdiegiamos, bet **neįkeliamos**

•

Programos, kurios įkeliamos, bet **nereaguoja**

Kitos programos

Be turinio politikos, kuri pateikta kitoje šio politikos centro dalyje, programoms, kurios sukurtos kitoms „Android“ sąsajoms ir yra platinamos per „Google Play“, taip pat gali būti taikomi konkrečių programų politikos reikalavimai. Peržiūrėkite toliau pateiktą sąrašą, kad nustatytumėte, ar šios politikos nuostatos taikomos jūsų programai.

„Android“ akimirksniu įkeliamos programos

„Android“ akimirksniu įkeliamų programų tikslas – teikti malonią, sklandžią naudotojo sąsają laikantis aukščiausių privatumo ir saugos standartų. Mūsų politika sukurta atsižvelgiant į šį tikslą.

Kūrėjai, kurie pasirenka platinti „Android“ akimirksniu įkeliamas programas per „Google Play“, turi laikytis toliau nurodytos politikos ir visų kitų [„Google Play“ kūrėjų programų politikos nuostatų](#).

Tapatybė

Naudodami akimirksniu įkeliamas programas su prisijungimo funkcija kūrėjai turi integruoti [„Smart Lock“](#), skirtą [slaptažodžiams](#) .

Nuorodų palaikymas

„Android“ akimirksniu įkeliamų programų kūrėjai turi tinkamai palaikyti kitų programų nuorodas. Jei kūrėjo akimirksniu įkeliamose programose arba įdiegtose programose yra nuorodų, kurios gali nukreipti į akimirksniu įkeliamą programą, kūrėjas turi nukreipti naudotojus į tą akimirksniu įkeliamą programą, o ne, pvz., užfiksuoti nuorodas naudodamas [žiniatinklio rodinį](#) .

Techninės specifikacijos

Kūrėjai turi laikytis „Google“ teikiamų „Android“ akimirksniu įkeliamų programų techninių specifikacijų ir reikalavimų (kurie gali būti retkarčiais keičiami), įskaitant pateiktus [viešuose dokumentuose](#) .

Programos įdiegimo siūlymas

Akimirksniu įkeliamose programose naudotojams gali būti siūloma įdiegiama programa, bet tai neturi būti pagrindinis akimirksniu įkeliamos programos tikslas. Siūlydami įdiegimą kūrėjai turi laikytis toliau pateiktų reikalavimų.

- Naudoti [trimačių objektų dizaino piktogramą „Gauti programą“](#) ir įdiegimo mygtuko etiketę „Įdiegti“.
- Akimirksniu įkeliamoje programoje neteikti daugiau nei 2–3 diegimo raginimų.
- Nenaudoti reklamjuostės ar kitų į skelbimus panašių technologijų naudotojams teikiant diegimo raginimus.

Išsamią akimirksniu įkeliamų programų informaciją ir NP gaires rasite straipsnyje apie [naudotojų patirties geriausios praktikos pavyzdžius](#).

Įrenginio būsenos keitimas

Akimirksniu įkeliamos programos negali atlikti naudotojo įrenginio pakeitimų, kurie išlieka ilgiau nei vyksta tokios programos seansas. Pvz., akimirksniu įkeliamos programos negali pakeisti naudotojo ekrano fono ar sukurti pagrindinio ekrano valdiklio.

Programos matomumas

Kūrėjai turi užtikrinti, kad akimirksniu įkeliamos programos matomos naudotojams, t. y. naudotojas turi visą laiką žinoti, kad akimirksniu įkeliamą programą veikia jo įrenginyje.

Įrenginių identifikatoriai

Akimirksniu įkeliamoms programoms neleidžiama pasiekti įrenginių identifikatorių, kurie 1) lieka, kai akimirksniu įkeliamą programą nustoja veikti, ir 2) kurių naudotojas negali nustatyti iš naujo. Pavyzdžiai (jais neapsiribojama)

- Versijos serijos numeris
- Tinklo lustų MAC adresai
- IMEI, IMSI

Akimirksniu įkeliamos programos gali pasiekti telefono numerį, jei jis gautas naudojant vykdymo laiko leidimą. Kūrėjas negali bandyti nustatyti naudotojo kontrolinio kodo naudodamas šiuos identifikatorius ar kitus būdus.

Tinklo srautas

Tinklo srautas iš akimirksniu įkeliamos programos turi būti šifruotas naudojant TLS protokolą, pvz., HTTPS.

„Android“ jaustukų politika

Mūsų jaustukų politika sukurta siekiant skatinti įtraukią ir nuoseklią naudotojų patirtį. Kad būtų galima tai įgyvendinti, visos programos turi palaikyti naujausios versijos [unikodo jaustukus](#), jei vykdomos 12 ar naujesnės versijos sistemoje „Android“.

Programos, kuriose naudojami numatytieji „Android“ jaustukai be jokių tinkintų diegimų, jau naudoja naujausios versijos unikodo jaustukus, jei vykdomos 12 ar naujesnės versijos sistemoje „Android“.

Programose su tinkintais jaustukų diegimais, įskaitant trečiosios šalies bibliotekų teikiamas programas, turi būti visiškai palaikoma naujausia unikodo versija, jei vykdoma 12 ar naujesnės versijos sistemoje „Android“, per keturis mėnesius nuo naujų unikodo jaustukų išleidimo datos.

Jei norite sužinoti, kaip palaikyti naujausius jaustukus, žr. šį [vadovą](#).

Šeimos

„Google Play“ kūrėjams teikia vertingą platformą, skirtą reklamuoti aukštos kokybės pagal amžių tinkamą turinį visai šeimai. Prieš pateikdami programą programoje „Skirta šeimai“ arba prieš pateikdami vaikams taikomą programą „Google Play“ parduotuvėje, turite užtikrinti, kad programa tinkama vaikams ir atitinka visus susijusius įstatymus.

[Sužinokite apie šeimų procesą ir peržiūrėkite interaktyvųjį kontrolinį sąrašą apsilankę puslapyje „Sėkmingo programėlių kūrimo mokymai“.](#)

„Google Play“ šeimos politika

Technologijos vis dažniau naudojamos kaip įrankis šeimos gyvenimui papildyti, todėl tėvai ieško saugaus, aukštos kokybės turinio, kurį galėtų bendrinti su vaikais. Nesvarbu, ar kuriate būtent vaikams skirtas programas ar jūsų programa gali tiesiog atkreipti vaikų dėmesį, „Google Play“ nori padėti užtikrinti, kad programa būtų saugi visiems naudotojams, įskaitant šeimas.

Žodžio „vaikai“ reikšmė gali skirtis skirtingose lokalėse ir esant skirtingam kontekstui. Svarbu pasitarti su savo teisininku, kuris padėtų nustatyti jūsų programai taikomus įsipareigojimus ir (arba) apribojimus pagal amžių. Jūs geriausiai žinote, kaip veikia jūsų programa, todėl pasitikime jumis ir tikime, kad padėsite užtikrinti šeimoms saugių programų teikimą sistemoje „Google Play“.

Galima pasirinkti, kad visos programos, kurios atitinka „Google Play“ šeimos politiką, būtų įvertintos pagal [mokytojų patvirtintą programą](#), bet negalime užtikrinti, kad jūsų programa bus įtraukta į mokytojų patvirtintą programą.

„Play Console“ reikalavimai

Tikslinė auditorija ir turinys

„Google Play Console“ skiltyje [„Tikslinė auditorija ir turinys“](#) prieš paskelbdami programą turite nurodyti tikslinę jos auditoriją pasirinkdami iš pateikto amžiaus grupių sąrašo. Neatsižvelgiant į tai, ką nurodysite sistemoje „Google Play Console“, jei pasirinksite į programą įtraukti vaizdų ir terminų, kurie gali būti laikomi taikomais vaikams, tai gali turėti įtakos „Google Play“ vertinant jūsų nurodytą tikslinę auditoriją. „Google Play“ pasilieka teisę atlikti programos informacijos, kurią pateikiate, peržiūrą savo nuožiūra, kad nustatytų, ar tiksliai nurodėte tikslinę auditoriją.

Daugiau nei vieną programos tikslinės auditorijos amžiaus grupę turėtumėte pasirinkti tik tuo atveju, jei programa skirta pasirinktos (-ų) amžiaus grupės (-ių) naudotojams ir įsitikinote, kad programa jiems tinkama. Pvz., jei programa skirta kūdikiams, pradedantiems vaikščioti ir ikimokyklinio amžiaus vaikams, kaip tikslinę šių programų amžiaus grupę turėtumėte pasirinkti tik „5 m. ir jaunesniems“. Jei programa skirta konkrečią klasę lankantiems vaikams, pasirinkite geriausiai šią klasę atitinkančią amžiaus grupę. Suaugusiuosius ir vaikus apimančias amžiaus grupes turėtumėte pasirinkti, tik jei jūsų programa tikrai skirta visoms amžiaus grupėms.

„Tikslinės auditorijos ir turinio“ skilties atnaujinimai

Galite bet kada atnaujinti programos informaciją „Google Play Console“ skiltyje „Tikslinė auditorija ir turinys“. Kad ši informacija būtų pateikta „Google Play“ parduotuvėje, būtina [atnaujinti programą](#). Tačiau bet kokie šioje „Google Play Console“ skiltyje atlikti pakeitimai gali būti peržiūrėti, ar atitinka politikos nuostatas, net prieš pateikiant programos naujinį.

Primygtinai rekomenduojame pranešti esamiems naudotojams, jei pakeičiate programos tikslinę amžiaus grupę ar pradodate naudoti skelbimus arba pirkimo programoje funkciją. Tai galite atlikti programos parduotuvės įrašo puslapio skiltyje „Kas naujo“ arba teikdami programos pranešimus.

Klaidinantis pristatymas sistemoje „Play Console“

Klaidinančiai pristačius bet kokią informaciją apie programą sistemoje „Play Console“, įskaitant skiltį „Tikslinė auditorija ir turinys“, programa gali būti pašalinta arba laikinai sustabdyta, todėl svarbu teikti tikslią informaciją.

Šeimos politikos reikalavimai

Jei viena iš tikslinių programos auditorijų yra vaikai, turite laikytis nurodytų reikalavimų. Nesilaikant šių reikalavimų programa gali būti pašalinta arba sustabdyta.

1. **Programos turinys:** vaikams pasiekiamas programos turinys turi būti tinkamas vaikams. Jei programoje yra turinio, kuris nėra visuotinai priimtinas, bet jis laikomas tinkamu naudotojams vaikams konkrečiame regione, programa gali būti pasiekama tame regione ([ribotuose regionuose](#)), bet bus nepasiekama kituose regionuose.
2. **Programos funkcijos:** programoje neturėtų būti teikiamas tik svetainės žiniatinklio rodinys arba jos pagrindinis tikslas neturėtų būti filialų srauto į svetainę pritraukimas be svetainės savininko ar administratoriaus leidimo.
3. **„Play Console“ atsakymai:** turite tiksliai atsakyti į klausimus apie programą sistemoje „Play Console“ ir atnaujinti šiuos atsakymus, kad tiksliai atspindėtų bet kokius programos pakeitimus. Tai apima (bet tuo neapsiriboja) tikslų atsakymų apie programą pateikimą tikslinės auditorijos ir turinio skiltyje, skiltyje „Duomenų sauga“ ir IARC turinio įvertinimo anketoje.
4. **Duomenų rinkimas, naudojimas ir apdorojimas:** turite paskelbti apie bet kokios vaikų [asmens ir neskkelbtinos informacijos](#) rinkimą programoje, įskaitant API ir SDK, išskviečiamus ar naudojamus programoje. Neskelbtina vaikų informacija apima (bet tuo neapsiribojama) autentifikavimo informaciją, mikrofono ir fotoaparato atpažinimo jutiklių duomenis, įrenginių duomenis, „Android“ ID ir skelbimų naudojimo duomenis. Taip pat turite užtikrinti, kad programoje laikomasi toliau nurodytų [duomenų rinkimo, naudojimo ir apdorojimo reikalavimų](#).
 - Programose, kurios taikomos tik vaikams, negalima perduoti „Android“ reklamavimo identifikatoriaus (angl. „Android advertising identifier“, AAID), SIM serijos numerio, versijos serijos numerio, PPRID, MAC, SSID, IMEI ir (arba) IMSI.
 - Programos, skirtos tik vaikams, neturėtų prašyti AD_ID leidimo, jei jos skirtos „Android API 33“ ar naujesnei programinei įrangai.
 - Programos, kurios taikomos vaikams ir vyresnėms auditorijoms, negali perduoti iš vaikų ar nežinomo amžiaus naudotojų gautų AAID, SIM serijos numerio, versijos serijos numerio, PPRID, MAC, SSID, IMEI ir (arba) IMSI.
 - Negalima prašyti įrenginio telefono numerio iš „Android“ API „TelephonyManager“.
 - Tik vaikams skirtos programos negali teikti užklausų dėl leidimo pasiekti vietovės duomenis arba rinkti, naudoti ir perduoti [tikslios vietovės](#).
 - Programos turi naudoti [„Companion Device Manager“ \(CDM\)](#) teikdamos „Bluetooth“ užklausą, nebent programa taikoma tik pagal įrenginio operacinės sistemos (OS) versijas, kurios nesuderinamos su CDM.
5. **API ir SDK:** turite užtikrinti, kad programoje tinkamai įdiegti bet kokie API ir SDK.
 - Programose, kurios taikomos tik vaikams, negali būti jokių API ar SDK, kurie nepatvirtinti naudoti vaikams skirtose paslaugose.
 - Pvz., API paslauga, naudojanti „OAuth“ technologijas autentifikavimo ir prieigos teisės suteikimo tikslais, kurios paslaugų teikimo sąlygose nurodyta, kad ji nėra patvirtinta naudoti vaikams skirtose paslaugose.
 - Vaikams ir vyresnei auditorijai taikomose programose negalima diegti API ar SDK, kurie nepatvirtinti naudoti vaikams skirtose paslaugose, nebent jie naudojami taikant [amžiaus filtrą](#) arba diegiami taip, kad nebūtų renkami duomenys iš vaikų. Programose, kurios taikomos vaikams ir vyresnėms auditorijoms, neturi būti reikalaujama, kad naudotojai pasiektų programos turinį naudodami API ar SDK, kuris nepatvirtintas naudoti vaikams skirtose paslaugose.

6. **Išplėstoji realybė (AR):** jei programoje naudojama išplėstoji realybė, turite įtraukti saugos įspėjimą, rodomą iš karto paleidžiant AR skiltį. Įspėjime turi būti pateikta toliau nurodyta informacija.

- Tinkamas pranešimas apie tėvų priežiūros svarbą.
- Priminimas, kad gali kilti fizinis pavojus realiame pasaulyje (pvz., kad naudotojai susipažintų su aplinka).
- Norint naudoti programą negali būti reikalaujama naudoti įrenginį, kurio nerekomenduojama naudoti vaikams (pvz., „Daydream“, „Oculus“).

7. **Socialinės programos ir funkcijos:** jei jūsų programose naudotojams leidžiama bendrinti informaciją ar ja keistis, turite aiškiai paskelbti šias funkcijas [turinio įvertinimo anketoje](#) sistemoje „Play Console“.

- Socialinės programos: socialinė programa – tai programa, kurios pagrindinis tikslas leisti naudotojams bendrinti laisvos formos turinį ar bendrauti su didelėmis žmonių grupėmis. Visose socialinėse programose, į kurių tikslinę auditoriją įtraukiami vaikai, turi būti pateiktas priminimas programoje, jog būtina užtikrinti saugą prisijungus ir saugotis pavojų realiame gyvenime, kurių gali kilti dėl sąveikų prisijungus, prieš leidžiant vaikams keistis laisvos formos medija ar informacija. Be to, prieš leidžiant vaikams keistis asmens informacija, turi būti reikalaujama, kad suaugęs asmuo atliktų tam tikrus veiksmus.
- Socialinės funkcijos: socialinė funkcija – tai bet kokia papildoma programos funkcija, leidžianti naudotojams bendrinti laisvos formos turinį ar bendrauti su didelėmis žmonių grupėmis. Bet kokiaje programoje, į kurios tikslinę auditoriją įtraukiami vaikai ir kurioje teikiamos socialinės funkcijos, turi būti pateiktas priminimas programoje, jog būtina užtikrinti saugą prisijungus ir saugotis pavojų realiame gyvenime, kurių gali kilti dėl sąveikų prisijungus, prieš leidžiant vaikams keistis laisvos formos medija ar informacija. Be to, turite pateikti metodą, kaip suaugusieji gali valdyti vaikams skirtas socialines funkcijas, įskaitant (bet tuo neapsiribojant) socialinės funkcijos įgalinimą ir (arba) išjungimą ar kitų funkcijų lygių pasirinkimą. Galiausiai, prieš įgalinant funkcijas, leidžiančias vaikams keistis asmens informacija, turi būti reikalaujama, kad suaugęs asmuo atliktų tam tikrus veiksmus.
- Suaugusiojo atliekamas veiksmas – tai mechanizmas, skirtas patvirtinti, kad naudotojas nėra vaikas ir vaikai nėra skatinami nurodyti klaidingą amžių, kad galėtų pasiekti tas programos sritis, kurios skirtos suaugusiems (t. y. suaugusiojo PIN kodas, slaptažodis, gimimo data, el. pašto patvirtinimas, asmens tapatybės dokumentas su nuotrauka, kredito kortelės informacija ar SSN).
- Socialinių programų, kurių pagrindinis tikslas yra bendravimas su nepažįstamais žmonėmis, negalima taikyti pagal vaikus. Pavyzdžiai: pokalbių ruletės stiliaus programos, pažinčių programos, vaikams skirtos atviros pokalbių patalpos ir kt.

8. **Teisinių reikalavimų laikymasis:** turite užtikrinti, kad programa, įskaitant visas API ar visus SDK, kuriuos programa iškviečia ar naudoja, atitinka [JAV vaikų privatumo ir apsaugos internete aktą \(angl. „U.S. Children’s Online Privacy and Protection Act“, COPPA\)](#) , [ES bendrąjį duomenų apsaugos reglamentą \(BDAR\)](#) ir bet kokius kitus taikytinus įstatymus ar nuostatas.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Programos, kurių parduotuvės įrašė reklamuojamas vaikams skirtas žaidimas, bet programos turinys tinkamas tik suaugusiems.
- Programos, kuriose įdiegiamos API, pagal kurių paslaugų teikimo sąlygas draudžiama jas naudoti vaikams skirtose programose.
- Programos, kuriose reklamuojamas alkoholio, tabako ar kontroliuojamų medžiagų vartojimas.
- Programos, apimančios realų arba imituojamą lošimą.
- Programos, kuriose yra smurtinio, šokiruojančio turinio ar kruvinų smurto scenų, netinkamos vaikams.
- Programos, teikiančios pažinčių paslaugas arba seksualinio pobūdžio ar su vedybiniu gyvenimu susijusius patarimus.

- Programos, kuriose yra nuorodų į svetaines, kuriose pateikiama turinio, pažeidžiančio „Google Play“
- Programos, kuriose vaikams rodomi suaugusiems skirti skelbimai (pvz., smurtinis, seksualinis, lošimo turinys).

Skelbimai ir pajamų gavimas

Jei gaunate pajamų iš programos, kuri taikoma pagal vaikus, sistemoje „Play“, programa turi atitikti toliau nurodytus šeimoms skirtų skelbimų ir pajamų gavimo politikos reikalavimus.

Toliau pateikta politika taikoma visiems pajamų gavimo ir reklamavimo elementams jūsų programoje, įskaitant skelbimus, reklamavimą įvairiose medijose (jūsų ir trečiųjų šalių programose), pirkimo programoje pasiūlymus ar bet kokią kitą komercinį turinį (pvz., rodant mokamus produktus). Visi pajamų gavimo ir reklamavimo elementai šiose programose turi atitikti visus galiojančius įstatymus ir nuostatus (įskaitant atitinkamus su savaiminiu reguliavimu susijusius principus ar pramonės gaires).

„Google Play“ pasilieka teisę atvesti, pašalinti ar sustabdyti programas, kuriose naudojami pernelyg agresyvūs komerciniai metodai.

Skelbimų reikalavimai

Jei programoje rodoma vaikams ar nežinomo amžiaus naudotojams skirtų skelbimų, turite:

- [„Google Play“ savarankiškai sertifikuotų skelbimų SDK šeimoms](#) naudoti tik siekdami rodyti skelbimus tiems naudotojams;
- užtikrinti, kad šiems naudotojams rodomuose skelbimuose nėra taikomas reklamavimas pagal pomėgius (reklamavimas, taikomas atskiriems naudotojams, turintiems tam tikrų savybių, atsižvelgiant į jų interneto naršymo elgseną) ar pakartotinė rinkodara (reklamavimas, taikomas atskiriems naudotojams pagal ankstesnę sąveiką su programa ar svetaine);
- užtikrinti, kad šiems naudotojams rodomuose skelbimuose teikiamas vaikams tinkamas turinys;
- užtikrinti, kad šiems naudotojams rodomi skelbimai atitinka šeimai skirtų skelbimų formato reikalavimus, ir
- užtikrinti, kad laikomasi visų galiojančių teisinių nuostatų ir pramonės standartų, susijusių su reklamavimu vaikams.

Skelbimo formato reikalavimai

Teikdami pajamų gavimo ir reklamavimo elementus programoje, negalite naudoti apgaulingo turinio ir jų negalima projektuoti taip, kad programą naudojantys vaikai atsitiktinai juos spustelėtų.

Jei vienintelė jūsų programos tikslinė auditorija yra vaikai, toliau nurodyti elementai draudžiami. Jei jūsų programos tikslinė auditorija yra vaikai ir vyresnė auditorija, toliau nurodyti elementai draudžiami, kai skelbimai teikiami vaikams ar nežinomo amžiaus naudotojams.

- Veikimą trikdančios pajamų gavimo ir reklamavimo elementai, įskaitant visą ekraną užimančius ar įprastą naudojimą trikdančius pajamų gavimo ir reklamavimo elementus, kai nesuteikiamas aiškus būdas atsisakyti skelbimo (pvz., [viso ekrano skelbimai](#)).
- Pajamų gavimo ir reklamavimo elementai, neleidžiantys įprastai naudoti programos ar žaisti žaidimo, įskaitant atlyginamus ar pasirenkamus skelbimus, kurių negalima uždaryti po penkių sekundžių.
- Pajamų gavimo ir reklamavimo elementai, kurie netrukdo įprastai naudoti programos ar žaisti žaidimo, gali būti rodomi ilgiau nei penkias sekundes (pvz., vaizdo įrašų turinys su integruotais skelbimais).
- Tarpinio puslapio pajamų gavimo ir reklamavimo elementai, pateikiami iš karto paleidus programą.
- Kelios skelbimų paskirties vietos puslapyje (pvz., neleidžiami reklamjuostės skelbimai, kuriuose rodomi keli pasiūlymai vienoje paskirties vietoje arba daugiau nei vienas reklamjuostės ar vaizdo įrašo skelbimas).

- Pajamų gavimo ir reklamavimo elementai, kurių negalima aiškiai atskirti nuo programos turinio, pvz., „Offerwall“ ir kitos įtraukiančių skelbimų funkcijos.
- Šokiruojančių ar emociškai veikiančių metodų naudojimas, norint paskatinti peržiūrėti skelbimus ar pirkti programose.
- Apgaulingi skelbimai, kuriuose naudotojas verčiamas spustelėti, naudojant atsisakymo mygtuką, kad būtų suaktyvintas kitas skelbimas, arba skelbimai, kurie staiga pasirodo programos srityse, kur naudotojas paprastai paliečia norėdamas naudoti kitą funkciją.
- Neatskiriamas virtualių žaidimo monetų ir realių pinigų naudojimas pirkiniams programoje.

Toliau pateikiami keli dažnai pasitaikančių pažeidimų pavyzdžiai.

- Pajamų gavimo ir reklamavimo elementai, kurie patraukiami naudotojui bandant juos uždaryti.
- Pajamų gavimo ir reklamavimo elementai, kuriuose naudotojui nesuteikiama galimybė išjungti pasiūlymo po penkių (5) sekundžių, kaip nurodyta toliau pateiktame pavyzdyje.

- Pajamų gavimo ir reklamavimo elementai, užimantys visą ekraną ar didžiąją jo dalį, ir naudotojui nepateikiamas aiškus būdas jų atsisakyti, kaip nurodyta toliau pateiktame pavyzdyje.

- Reklamjuosčių skelbimai, kuriuose rodomi keli pasiūlymai, kaip nurodyta toliau pateiktame pavyzdyje.

- Pajamų gavimo ir reklamavimo elementai, kuriuos naudotojas gali palaikyti programos turiniu, kaip nurodyta toliau pateiktame pavyzdyje.



- Mygtukai, skelbimai ar kiti pajamų gavimo elementai, kuriuose reklamuojami kiti jūsų „Google Play“ parduotuvės įrašai, bet kurių negalima atskirti nuo programos turinio, kaip nurodyta toliau

pateiktame pavyzdyje.

Pateikiami keli netinkamo skelbimų turinio, kurio negalima teikti vaikams, pavyzdžiai.

- **Netinkamas medijos turinys:** TV serialų, filmų, muzikos albumų ar bet kokios kitos medijos, kuri nėra tinkama vaikams, skelbimai.
- **Netinkami vaizdo žaidimai ir atsisiunčiama programinė įranga:** atsisiunčiamos programinės įrangos ir elektroninių vaizdo žaidimų skelbimai, kurie nėra tinkami vaikams.

- **Kontroliuojamos arba žalingos medžiagos:** alkoholio, tabako, kontroliuojamų ar kitų žalingų medžiagų skelbimai.
- **Lošimas:** imituojamo lošimo, varžybų ar lažybų žirgų lenktynėse skelbimai, net jei įėjimas nemokamas.
- **Suaugusiesiems skirtas ir seksualinio pobūdžio turinys:** skelbimai su seksualiniu ir suaugusiesiems skirtu turiniu.
- **Pasimatymai ir santykiai:** pasimatymų ar suaugusiųjų santykių svetainių skelbimai.
- **Smurtinis turinys:** skelbimai, kuriuose yra smurtinio ir atviro turinio, netinkamo vaikams.

Skelbimų SDK

Jei programoje teikiate skelbimų, o tikslinė auditorija apima tik vaikus, turite naudoti tik [savarankiškai sertifikuotų skelbimų SDK šeimoms](#) versijas. Jei į programos tikslinę auditoriją įtraukiami vaikai ir vyresni naudotojai, turite naudoti amžiaus tikrinimo priemones, pvz., [amžiaus filtrą](#), ir užtikrinti, kad vaikams rodomi skelbimai teikiami tik iš „Google Play“ savarankiškai sertifikuotų skelbimų SDK versijų.

Jei reikia išsamesnės informacijos apie šiuos reikalavimus, žr. [savarankiškai sertifikuotų skelbimų SDK programos šeimoms politikos](#) puslapį, o jei norite peržiūrėti dabartinį savarankiškai sertifikuotų skelbimų SDK šeimoms versijų sąrašą, žr. [čia](#).

Jei naudojate „AdMob“, daugiau informacijos apie produktus žr. [„AdMob“ pagalbos centre](#).

Jūs privalote užtikrinti, kad programa atitiktų visus reikalavimus, susijusius su skelbimais, pirkimu programoje ir komerciniu turiniu. Jei norite sužinoti daugiau apie turinio politiką ir reklamavimo praktikos metodus, susisiekite su skelbimų SDK teikėju (-ais).

Savarankiškai sertifikuotų skelbimų SDK politika šeimoms

„Google Play“ yra įsipareigojusi kurti saugią patirtį vaikams ir šeimoms. Svarbiausia, kad vaikai matytų tik jų amžiui tinkamus skelbimus ir kad jų duomenys būtų tinkamai tvarkomi. Siekdami šio tikslo reikalaujame, kad skelbimų SDK ir tarpininkavimo platformos savarankiškai patvirtintų, kad yra tinkamos vaikams ir atitinka [„Google Play“ kūrėjų programos politiką](#) bei [„Google Play“ šeimos politiką](#), įskaitant [Savarankiškai sertifikuotų skelbimų SDK programos šeimoms reikalavimus](#).

„Google Play“ savarankiškai sertifikuotų skelbimų SDK programa šeimoms yra svarbus būdas kūrėjams nustatyti, kurie skelbimų SDK ar tarpininkavimo platformos savarankiškai patvirtino, kad yra tinkami naudoti specialiai vaikams skirtose programose.

Klaidinančiai pristačius bet kokią informaciją apie SDK, įskaitant [susidomėjimo formos](#) paraiškoje, SDK gali būti laikinai sustabdytas ar pašalintas iš Savarankiškai sertifikuotų skelbimų SDK programos šeimoms, todėl svarbu pateikti tikslią informaciją.

Politikos reikalavimai

Jei jūsų SDK arba tarpininkavimo platforma yra skirta programoms, įtrauktoms į „Google Play“ programą „Skirta šeimai“, privalote laikytis visų „Google Play“ politikos programų kūrėjams reikalavimų, įskaitant pateiktus toliau. Neįvykdę kurių nors politikos reikalavimų, galite būti visam laikui ar laikinai pašalinti iš Savarankiškai sertifikuotų skelbimų SDK programos šeimoms.

Privalote užtikrinti, kad jūsų SDK ar tarpininkavimo platforma atitiktų reikalavimus, todėl būtinai perskaitykite [„Google Play“ kūrėjų programos politiką](#), [„Google Play“ šeimos politiką](#) ir [Savarankiškai sertifikuotų skelbimų SDK programos šeimoms reikalavimus](#).

1. **Skelbimo turinys:** vaikams pasiekiamas skelbimo turinys turi būti tinkamas vaikams.
 - Privalote (i) apibrėžti nepriimtina skelbimo turinį bei veiksmus ir (ii) drausti juos savo taisyklėse ar politikoje. Apibrėžtys turi atitikti [„Google Play“ kūrėjų programos politiką](#).
 - Taip pat privalote sukurti skelbimų failų vertinimo pagal konkretaus amžiaus grupės metodą. Konkretaus amžiaus grupės turi apimti bent grupes „Visiems“ ir „Suaugusiesiems“. Vertinimo

metodai turi atitikti metodus, kuriuos „Google“ teikia SDK, kai kūrėjai užpildo [susidomėjimo formą](#)

- Privalote užtikrinti, kad tais atvejais, kai skelbimai vaikams teikiami naudojant kainų siūlymą realiuoju laiku, skelbimo failai būtų peržiūrėti ir atitiktų pirmiau nurodytus reikalavimus.
 - Be to, privalote turėti [mechanizmą, pagal kurį vizualiai atpažintumėte, kad skelbimo failai](#) yra iš jų skelbimų vietų (pavyzdžiui, pažymėkite skelbimo failą savo įmonės logotipo ar panašios funkcijos vandens ženklu).
2. **Skelbimo formatas:** privalote užtikrinti, kad visi vaikams naudotojams rodomi skelbimai atitiktų šeimai skirtų skelbimų formato reikalavimus, ir leisti kūrėjams pasirinkti skelbimų formatus, atitinkančius [„Google Play“ šeimos politiką](#).
- Skelbimuose negalite naudoti apgaulingo turinio ir jų negalima kurti taip, kad programą naudojantys vaikai atsitiktinai juos spustelėtų. Apgaulingi skelbimai, kuriuose naudotojas verčiamas spustelėti, naudojant atsakymo mygtuką, kad būtų suaktyvintas kitas skelbimas, arba skelbimai, kurie staiga pasirodo programos srityse, kur naudotojas paprastai paliečia norėdamas naudoti kitą funkciją, neleidžiami.
 - Negalite naudoti trikdančių skelbimų, įskaitant skelbimus, kurie užima visą ekraną ar trukdo įprastai naudoti ir nesuteikia aiškios priemonės, kaip atsakyti skelbimo (pvz., [viso ekrano skelbimų](#)).
 - Skelbimus, kurie trukdo įprastai naudotis programa ar žaisti žaidimą, įskaitant atlyginamus ar pasirenkamus skelbimus, turi būti galima uždaryti po penkių sekundžių.
 - Kelios skelbimo paskirties vietos puslapyje neleidžiamos. Pavyzdžiui, neleidžiami reklamjuostės skelbimai, kuriuose rodomi keli pasiūlymai vienoje paskirties vietoje arba daugiau nei vienas reklamjuostės ar vaizdo įrašo skelbimas.
 - Skelbimai turi būti lengvai atskiriami nuo programos turinio. „Offerwall“ ir įtraukiančių skelbimų funkcijos, kurių naudotojai vaikai negali aiškiai identifikuoti kaip reklamavimo, neleidžiamos.
 - Skelbimuose negalima naudoti šokiruojančių ar emociškai veikiančių metodų, norint paskatinti peržiūrėti skelbimus.
3. **RPP / pakartotinė rinkodara:** privalote užtikrinti, kad vaikams naudotojams pateikiamuose skelbimuose nėra taikomas reklamavimas pagal pomėgius (reklamavimas, taikomas atskiriems naudotojams, turintiems tam tikrų savybių, atsižvelgiant į jų interneto naršymo elgseną) ar pakartotinė rinkodara (reklamavimas, taikomas atskiriems naudotojams pagal ankstesnę sąveiką su programa ar svetaine).
4. **Duomenų rinkimas, naudojimas ir apdorojimas:** jūs, SDK teikėjas, privalote skaidriai tvarkyti naudotojo duomenis (pavyzdžiui, iš naudotojo arba apie naudotoją surinktą informaciją, įskaitant informaciją apie įrenginį). Tai reiškia, kad turite aiškiai paskelbti, jog jūsų SDK pasiekia, renka, naudoja ir bendrina duomenis, ir juos naudoti tik nurodytais tikslais. Šie „Google Play“ reikalavimai papildo bet kokius taikomuose privatumo ir duomenų apsaugos įstatymuose numatytus reikalavimus. Privalote atskleisti, kad renkama bet kokia [asmens ir neskkelbtina informacija](#) iš vaikų, įskaitant autentifikavimo informaciją, mikrofono ir kamerų atpažinimo jutiklių duomenis, įrenginio duomenis, „Android ID“ ir skelbimų naudojimo duomenis, bet tuo neapsiribojant.
- Privalote leisti leidėjams (pateikus užklausą ar naudojant programą) teikti užklausas dėl skelbimų teikimo vaikams skirtame turinyje. Toks turinys turi atitikti galiojančius įstatymus ir nuostatus, pvz., [JAV vaikų privatumo ir apsaugos internete aktą \(angl. „Children’s Online Privacy and Protection Act“, COPPA\)](#) ir [ES bendrąjį duomenų apsaugos reglamentą \(BDAR\)](#).
 - „Google Play“ reikalauja skelbimų SDK išjungti suasmenintus skelbimus, reklamavimą pagal pomėgius ir pakartotinę rinkodarą kaip vaikams skirtą turinio dalį.
 - Privalote užtikrinti, kad, kai skelbimai vaikams rodomi naudojant kainų siūlymą realiuoju laiku, kainų siūlytojams taikomi privatumo rodikliai.
 - Negalite perduoti iš vaikų ar nežinomo amžiaus naudotojų gautų AAID, SIM serijos numerio, versijos serijos numerio, PPRID, MAC, SSID, IMEI ir (arba) IMSI.

5. **Tarpininkavimo platformos:** kai teikiate skelbimus vaikams, privalote laikytis toliau pateiktų reikalavimų.
- Turi būti naudojami tik savarankiškai sertifikuoti skelbimų SDK šeimoms arba taikomos apsaugos priemonės, kuriomis būtų užtikrinta, kad visi iš tarpininkavimo tinklų teikiami skelbimai atitinka šiuos reikalavimus.
 - Perduokite informaciją, reikalingą tarpininkavimo platformoms, norint nurodyti skelbimo turinio įvertinimą ir bet kokią taikomą vaikams skirtą turinį.
6. **Savarankiškas sertifikavimas ir atitiktis:** turite pateikti „Google“ pakankamai informacijos, pvz., [susidomėjimo formoje](#) nurodytos informacijos, kad būtų galima patikrinti, ar skelbimų SDK politika atitinka visus savarankiško sertifikavimo reikalavimus, įskaitant nurodytus toliau, bet jais neapsiribojant.
- Pateikite savo SDK arba tarpininkavimo platformos paslaugų teikimo sąlygų, privatumo politikos ir leidėjo integracijos vadovo versiją anglų kalba.
 - Pateikite [pavyzdinę bandomąją programą](#), kurioje naudojama naujausia reikalavimus atitinkanti skelbimų SDK versija. Pavyzdinė bandomoji programa turėtų būti visiškai sukurta ir vykdomas „Android“ APK, kuriame naudojamos visos SDK funkcijos. Bandomosios programos reikalavimai
 - Ji turi būti pateikta kaip visiškai sukurta ir vykdomas „Android“ APK, skirtas vykdyti naudojant telefono formos koeficientą.
 - Joje turi būti naudojama naujausia išleista arba netrukus pasirodysianti skelbimų SDK versija, atitinkanti „Google Play“ politiką.
 - Joje turi būti naudojamos visos skelbimų SDK funkcijos, įskaitant skelbimų SDK iškvietimą, kad būtų galima gauti ir pateikti skelbimus.
 - Jai turi būti suteikta visateisė prieiga prie visų aktyvių ir (arba) teikiamų skelbimų vietų tinkle, naudojant skelbimų failus, kurių užklausa pateikiama per bandomąją programą.
 - Ji negali būti apribota pagal geografinę vietovę.
 - Jei skelbimų vietos skirtos mišriai auditorijai, bandomojoje programoje turi būti galima atskirti skelbimų failų iš visų skelbimų vietų ir skelbimų vietų, tinkamų vaikams arba visoms amžiaus grupėms, užklausa.
 - Ji negali būti ribojama konkrečioms skelbimų vietų skelbimams, nebent jai taikomas amžiaus filtras.
7. Privalote laiku atsakyti į visus vėlesnius prašymus pateikti informaciją ir [savarankiškai sertifikuoti](#) , kad visos naujai išleistos versijos atitiktų naujausias „Google Play“ kūrėjų programos politikos nuostatas, įskaitant šeimos politikos reikalavimus.
8. **Teisinių reikalavimų laikymasis:** savarankiškai sertifikuotų skelbimų SDK šeimoms turi palaikyti skelbimų teikimą, atitinkantį visus su vaikais susijusius įstatymus ir reglamentus, kurie gali būti taikomi jų leidėjams.
- Privalote užtikrinti, kad jūsų SDK arba tarpininkavimo platforma atitiktų [JAV vaikų privatumo ir apsaugos internete aktą \(angl. „U.S. Children's Online Privacy and Protection Act“, COPPA\)](#) , [ES bendrąjį duomenų apsaugos reglamentą \(BDAR\)](#) ir visus kitus taikytinus įstatymus ar reglamentus.

Pastaba: žodžio „vaikai“ reikšmė gali skirtis skirtingose lokalėse ir esant skirtingam kontekstui. Svarbu pasitarti su teisininku, kuris padėtų nustatyti programai taikomus įsipareigojimus ir (arba) apribojimus pagal amžių. Jūs patys geriausiai žinote, kaip veikia jūsų programa, todėl pasitikime jumis ir tikime, kad padėsite užtikrinti šeimoms saugią programų teikimą sistemoje „Google Play“.

Jei reikia daugiau informacijos apie programos reikalavimus, žr. [savarankiškai sertifikuotų skelbimų SDK programos šeimoms](#) puslapį.

Visada geriau išvengti pažeidimo nei bandyti jį pašalinti, bet kai politika pažeidžiama, stengiamės užtikrinti, kad kūrėjai supranta, kaip gali sutvarkyti programą, kad ji atitiktų politiką. Praneškite mums, jei [pastebėsite pažeidimų](#) ar kils klausimų apie [pažeidimo tvarkymą](#).

Politikos aprėptis

Mūsų politika taikoma bet kokiam turiniui, kuris pateikiamas programoje ar su kuriuo ji susieta, įskaitant skelbimus, kurie rodomi naudotojams, ir naudotojų sukurtą turinį, kuris priglobiamas programoje ar su kuriuo ji susieta. Be to, ji taikoma bet kokiam turiniui iš kūrėjo paskyros, kuris viešai pateikiamas „Google Play“, įskaitant kūrėjo vardą ir nurodytos kūrėjo svetainės nukreipimo puslapį.

Neleidžiame teikti programų, kuriose naudotojams leidžiama į įrenginį įdiegti kitų programų. Programose, kuriose galima pasiekti kitas programas, žaidimus ar programinę įrangą jų neįdiegiant, įskaitant trečiųjų šalių teikiamas funkcijas ir turinį, turi būti užtikrinama, kad visas turinys, kurį jose galima pasiekti, atitiktų visą „Google Play“ politiką, o šioms programoms taip pat gali būti taikoma papildoma politikos peržiūra.

Šiose politikos nuostatose naudojami terminai reiškia tą patį, kaip nurodyta [Kūrėjų platinimo sutartyje](#) (KPS). Privalote ne tik laikytis šios politikos ir KPS, bet ir įvertinti programos turinį vadovaudamiesi [turinio vertinimo gairėmis](#).

Neleidžiame teikti programų ar programų turinio, kuriuo kenkiama naudotojų pasitikėjimui „Google Play“ ekosistemoje. Vertindami, ar įtraukti programas į „Google Play“, ar jas pašalinti, atsižvelgiame į įvairius veiksnius, įskaitant žalingą elgseną ar didelę piktnaudžiavimo riziką (bet tuo neapsiribojant). Piktnaudžiavimo riziką nustatome pagal tam tikrus elementus, pavyzdžiui, konkrečių programų ir kūrėjų skundus, naujienų pranešimus, ankstesnių pažeidimų istoriją, naudotojų atsiliepimus ir populiarų prekės ženklą, simbolių bei kitų išteklių naudojimą (bet jais neapsiribojame).

Kaip veikia „Google Play Protect“

„Google Play Protect“ tikrina programas, kai jas įdiegiate. Be to, ji periodiškai nuskaito jūsų įrenginį. Jei randa potencialiai žalingą programą, ji gali:

- siųsti pranešimą. Kad pašalintumėte programą, palieskite pranešimą, tada – „Pašalinti“;
- išjungti programą, kol ją pašalinsite;
- automatiškai pašalinti programą. Daugeliu atvejų, jei aptinkama žalinga programa, galite gauti pranešimą, kuriame nurodoma, kad programa pašalinta.

Kaip veikia apsauga nuo kenkėjiškų programų

Siekdama apsaugoti jus nuo kenkėjiškos trečiųjų šalių programinės įrangos, URL ir kitų saugos problemų, „Google“ gali gauti informacijos apie:

- jūsų įrenginio tinklo ryšius;
- potencialiai žalingus URL;
- operacinę sistemą ir programas, kurias įdiegėte įrenginyje iš „Google Play“ arba kitų šaltinių.

Galite iš „Google“ gauti įspėjimą apie galbūt nesaugią programą arba URL. „Google“ gali pašalinti tokią programą arba URL ar neleisti jų įdiegti, jei yra žinoma, kad jie kenkia įrenginiams, duomenims arba naudotojams.

Galite išjungti kai kurias iš šių apsaugos priemonių įrenginio skiltyje „Nustatymai“. Bet „Google“ gali toliau gauti informacijos apie programas, įdiegtas iš „Google Play“, ir programos, įdiegtos įrenginyje iš kitų šaltinių, gali būti toliau analizuojamos ieškant saugos problemų, bet nesiunčiant informacijos į sistemą „Google“.

Kaip veikia privatumo įspėjimai

„Google Play Protect“ įspės jus, jei programa bus pašalinta iš „Google Play“ parduotuvės, nes programa gali pasiekti jūsų asmens informaciją, ir galėsite pašalinti programą.

Vykdymo procesas

Kai peržiūrite turinį ar paskyras norėdami nustatyti, ar jie neteisėti arba pažeidžia mūsų politiką, priimdami sprendimą atsižvelgiame į įvairią informaciją, įskaitant programos metaduomenis (pvz., programos pavadinimą, aprašą), funkcijas programoje, paskyros informaciją (pvz., ankstesnę politikos pažeidimų istoriją) ir kitą informaciją, teikiamą naudojant ataskaitų teikimo mechanizmus (jei taikoma) ir mūsų pačių inicijuotas apžvalgas.

Jei programa ar kūrėjo paskyra pažeidžia bet kurią politikos nuostatą, imsime atitinkamų veiksmų, kaip nurodyta toliau. Be to, pateiksime atitinkamą informaciją apie atliktą veiksmą el. paštu ir instrukcijas, kaip pateikti apeliaciją, jei manote, kad ėmėmės veiksmų per klaidą.

Atminkite, kad pašalinimo ar administraciniuose pranešimuose gali būti nurodyti ne visi politikos pažeidimai, aptikti jūsų paskyroje, programoje ar išsamesniame programų kataloge. Kūrėjai privalo imtis veiksmų dėl bet kokios politikos problemos ir tinkamai vykdyti papildomas pareigas, kad užtikrintų, jog likusi programos ar paskyros dalis atitinka visas politikos nuostatas. Jei nepašalinsite politikos pažeidimų paskyroje ir visose programose, gali būti imtasi papildomų įgyvendinimo veiksmų.

Jei bus pasikartojančių ar rimtų šios politikos nuostatų ar [Kūrėjų platinimo sutarties](#) (KPS) pažeidimų (pvz., kenkėjiškos programos, apgaulė ir programos, kurios kenkia naudotojui ar įrenginiui), asmeninės ar susijusios „Google Play“ kūrėjų paskyros bus nutrauktos.

Įgyvendinimo veiksmai

Skirtingi įgyvendinimo veiksmai gali skirtingai paveikti programas. Naudojame automatizuotą ir žmonių atliekamą vertinimą peržiūrėdami programas ir programų turinį, siekdami aptikti ir įvertinti turinį, kuris pažeidžia mūsų politiką ir yra žalingas naudotojams bei bendrajai „Google Play“ ekosistemai. Naudodami automatizuotus modelius galime lengviau aptikti daugiau pažeidimų ir sparčiau įvertinti potencialias problemas, taip visiems užtikrindami „Google Play“ saugą. Politiką pažeidžiantis turinys pašalinamas taikant automatizuotus modelius arba, jei reikalingas subtilesnis sprendimas, pažymimas, kad vertinimus atliekantys išmokyti operatoriai ir analitikai atliktų išsamesnę peržiūrą, pvz., jei reikia atsižvelgti į turinio dalies kontekstą. Šių neautomatiškai atliktų peržiūrų rezultatai naudojami mokymo duomenims kaupti ir mašininio mokymosi modeliams toliau tobulinti.

Toliau pateiktoje skiltyje aprašomi įvairūs veiksmai, kuriuos gali atlikti „Google Play“, ir poveikis programai ir (arba) „Google Play“ kūrėjo paskyrai.

Šie veiksmai taikomi visuose regionuose, jei nenurodyta kitaip įgyvendinimo pranešimuose. Pvz., jei programa laikinai sustabdyta, ji bus nepasiekiamą visuose regionuose. Be to, jei nenurodyta kitaip, šie veiksmai liks galioti, nebent pateiksite apeliaciją dėl veiksmo ir ji bus patenkinta.

Atmetimas

- Peržiūrėti pateikta nauja programa arba programos naujins nebus pasiekiami sistemoje „Google Play“.
- Jei esamos programos naujins buvo atmetas, prieš naujinį paskelbta programos versija vis tiek bus pasiekiamą sistemoje „Google Play“.
- Atmetimas neturi įtakos prieigai prie esamų atmetos programos naudotojų diegimų, statistikos ir įvertinimų.
- Atmetimas neturi įtakos „Google Play“ kūrėjo paskyros būsenai.

Pastaba: nebandykite iš naujo pateikti atmetos programos, jei nepašalinsite visų politikos pažeidimų.

Pašalinimas

- Programa su visomis ankstesnėmis jos versijomis pašalinama iš „Google Play“ ir naudotojai jos nebegali atsisiųsti.
- Kadangi programa pašalinama, naudotojai negali peržiūrėti programos parduotuvės įrašo. Ši informacija bus atkurta, kai pateiksite pašalintos programos politiką atitinkantį naujinį.
- Naudotojams gali būti neleidžiama pirkti programoje ar naudoti bet kokių pirkimo programoje atsiskaitant per „Google Play“ funkcijų programoje, kol „Google Play“ patvirtins politikos nuostatas atitinkančią versiją.
- Pašalinimai iškart nepaveikia „Google Play“ kūrėjo paskyros būsenos, tačiau dėl kelių pašalinių paskyra gali būti sustabdyta.

Pastaba: nebandykite iš naujo paskelbti pašalintos programos, kol išspręsite visus politikos pažeidimus.

Sustabdymas

- Programa su visomis ankstesnėmis jos versijomis pašalinama iš „Google Play“ ir naudotojai jos nebegali atsisiųsti.
- Sustabdyta gali būti dėl rimtų ar kelių politikos pažeidimų, taip pat dėl pakartotinių programos atmetimų ar pašalinių.
- Kadangi programa sustabdyta, naudotojai negalės matyti programos parduotuvės įrašo.
- Nebegalite naudoti laikinai sustabdytos programos APK ar programos komponentų rinkinio.
- Naudotojams nebus leidžiama pirkti programoje ar naudoti bet kokių pirkimo programoje atsiskaitant per „Google Play“ funkcijų programoje.
- Sustabdytas laikomas įspėjimu ir pablogina gerą „Google Play“ kūrėjo paskyros būseną. Gavus kelis įspėjimus asmeninės ir susijusios „Google Play“ kūrėjų paskyros gali būti nutrauktos.

Ribotas matomumas

- Programos aptinkamumas sistemoje „Google Play“ apribotas. Programa išliks pasiekiamą sistemoje „Google Play“ ir ją galės pasiekti naudotojai, turintys tiesioginę nuorodą į programos parduotuvės įrašą.
- Riboto matomumo būsenos programos nustatymas neturi įtakos „Google Play“ kūrėjo paskyros būsenai.
- Programos riboto matomumo būsenos nustatymas neturi įtakos naudotojų galimybei peržiūrėti esamą programos parduotuvės įrašą.

Ribojami regionai

- Jūsų programą sistemoje „Google Play“ gali atsisiųsti tik naudotojai tam tikruose regionuose.
- Naudotojai iš kitų regionų negalės surasti programos „Play“ parduotuvėje.
- Anksčiau programą įdiegę naudotojai gali toliau ją naudoti savo įrenginiuose, bet nebegaus naujinių.
- Ribojimas pagal regionus neturi įtakos jūsų „Google Play“ kūrėjo paskyros būsenai.

Apribotos paskyros būseną

- Kai kūrėjo paskyra bus apribotos būsenos, visos kataloge esančios programos bus pašalintos iš „Google Play“ ir nebegalėsite skelbti naujų ar iš naujo skelbti esamų programų. Vis tiek galėsite pasiekti „Play Console“.
- Kadangi visos programos pašalinamos, naudotojai negalės peržiūrėti jūsų programos parduotuvės įrašo ir kūrėjo profilio.
- Dabartiniais naudotojams nebus leidžiama pirkti programoje ar naudoti bet kokių pirkimo programoje atsiskaitant per „Google Play“ funkcijų programoje.

- Vis tiek galite naudoti „Play Console“ norėdami pateikti daugiau informacijos sistemoje „Google Play“ ir taisyti paskyros informaciją.
- Pašalinę visus politikos pažeidimus galėsite iš naujo paskelbti programas.

Paskyros nutraukimas

- Kai kūrėjo paskyra bus nutraukta, visos kataloge esančios programos bus pašalintos iš „Google Play“ ir nebegalėsite skelbti naujų programų. Be to, tai reiškia, kad visos susijusios „Google Play“ kūrėjų paskyros taip pat bus visam laikui sustabdytos.
- „Play Console“ paskyra gali būti nutraukta dėl kelių sustabdymų ar sustabdymų dėl rimtų politikos pažeidimų.
- Kadangi programos paskyroje, kurios teikimas nutrauktas, pašalinamos, naudotojai negalės matyti programų parduotuvės įrašo ir kūrėjo profilio.
- Dabartiniais naudotojams nebus leidžiama pirkti programoje ar naudoti bet kokių pirkimo programoje atsiskaitant per „Google Play“ funkcijų programoje.

Pastaba: bet kokia nauja paskyra, kurią bandysite atidaryti, taip pat bus nutraukta (negrąžinus kūrėjo registracijos mokesčio), todėl nebandykite registruotis gauti naują „Play Console“ paskyrą, kol nutraukta viena iš jūsų paskyrų.

Nenaudojamos paskyros

Nenaudojamos paskyros – tai kūrėjų paskyros, kurios yra neaktyvios ar kurių naudojimas yra nutrauktas. Nenaudojamų paskyrų būsenos negalima laikyti gera, kaip to reikalaujama [Kūrėjų platinimo sutartyje](#).

„Google Play“ kūrėjų paskyros skirtos aktyviems kūrėjams, kurie paskelbia ir aktyviai prižiūri programas. Siekdami išvengti piktnaudžiavimo, uždarome paskyras, kurios nėra reguliariai naudojamos arba kitaip glaudžiai susijusios su programų paskelbimu ir atnaujinimu, statistikos pasiekiamumu arba parduotuvių įrašų valdymu.

[Uždariant nenaudojamą paskyrą](#) ištrinama paskyra ir visi su ja susieti duomenys. Registracijos mokestis negrąžinamas ir bus išskaitytas. Prieš uždarydami nenaudojamą paskyrą, įspėsime jus pasinaudodami jūsų pateikta kontaktine informacija, susijusia su ta paskyra.

Nors nenaudojama paskyra uždaroma, ateityje galėsite sukurti naują paskyrą, jei nuspręsite paskelbti sistemoje „Google Play“. Negalėsite iš naujo suaktyvinti savo paskyros, o ankstesnės programos ar duomenys nebus pasiekiami naujoje paskyroje.

Politikos nuostatų pažeidimų tvarkymas ir pranešimas apie juos

Apeliacija dėl įgyvendinimo veiksmo

Programas atkursime tais atvejais, jei įvyks klaida ir bus nustatyta, kad programa nepažeidžia „Google Play“ programų politikos ir Kūrėjų platinimo sutarties. Jei atidžiai peržiūrėjote politiką ir manote, kad sprendimas galėjo būti klaidingas, vadovaukitės įgyvendinimo el. pašto pranešime pateiktomis instrukcijomis arba [spustelėkite čia](#), kad pateiktumėte apeliaciją dėl sprendimo.

Papildomi ištekliai

Jei reikia daugiau informacijos apie įgyvendinimo veiksmą arba naudotojo pateiktą įvertinimą ir (arba) komentarą, peržiūrėkite toliau pateiktus šaltinius arba susisiekite su mumis apsilankę . Tačiau negalime patarti teisiniais klausimais. Jei reikia teisinių patarimų, susisiekite su teisininku.

- [Programos patvirtinimas](#)
- [Pranešimas apie politikos nuostatų pažeidimą](#)

- [Susisiekimasis su „Google Play“ dėl paskyros uždarymo arba programos pašalinimo](#)
 - [Sąžiningi įspėjimai](#)
 - [Pranešimas apie netinkamus komentarus ir programas](#)
 - [Mano programa buvo pašalinta iš sistemos „Google Play“](#)
 - [Apie „Google Play“ kūrėjų paskyrų nutraukimą](#)
-

„Play Console“ reikalavimai

Siekdama užtikrinti savo gyvybingos programų ekosistemos saugą ir saugumą, „Google Play“ reikalauja, kad visi kūrėjai atitiktų „Play Console“ reikalavimus, įskaitant visus profilius, kurie yra susieti su „Play Console“ kūrėjo paskyra. „Google Play“ sistemoje bus rodoma patikrinta informacija, kad naudotojai galėtų pasitikėti kūrėjais. Sužinokite daugiau apie [informaciją, rodomą sistemoje „Google Play“](#).

„Google Play“ teikiamos dviejų tipų kūrėjo paskyros: asmeninės ir organizacijos. Norint užtikrinti sklandų naujų partnerių priėmimo procesą, labai svarbu pasirinkti tinkamą kūrėjo paskyros tipą ir atlikti reikiamus patvirtinimo veiksmus. Sužinokite daugiau apie [kūrėjo paskyros tipo pasirinkimą](#).

Kurdami „Play Console“ kūrėjo paskyrą, kūrėjai, teikiantys toliau nurodytas paslaugas, turi užsiregistruoti kaip organizacija.

- Finansiniai produktai ir paslaugos, įskaitant banko paslaugas, paskolų teikimą, prekybą akcijomis, investicinius fondus, kriptovaliutų programines pinigines ir kriptovaliutos keityklas (bet tuo neapsiribojant). Sužinokite daugiau apie [finansinių paslaugų politiką](#).
- Sveikatos programos, pvz., medicinos programos ir su žmonėmis susijusių tyrimų programos. Sužinokite daugiau apie [sveikatos programų kategorijas](#).
- Programos, patvirtintos naudoti [VPN paslaugos](#) klasę. Sužinokite daugiau apie [VPN paslaugos politiką](#).
- Valstybės institucijų programos, įskaitant programas, sukurtas vyriausybės įstaigos arba jos vardu.

Pasirinkę paskyros tipą privalote atlikti toliau nurodytus veiksmus.

- Tiksliai pateikite kūrėjo paskyros informaciją, įskaitant toliau nurodytą išsamią informaciją.
 - Juridinis pavadinimas ir adresas
 - [DUNS numeris](#) , jei užregistruota kaip organizacija
 - Kontaktinis el. pašto adresas ir telefono numeris
 - Kūrėjo el. pašto adresas ir telefono numeris, rodomi sistemoje „Google Play“, jei taikoma
 - Mokėjimo metodai, jei taikoma
 - „Google“ mokėjimų profilis, susietas su kūrėjo paskyra
- Jei registruojatės kaip organizacija, įsitikinkite, kad jūsų kūrėjo paskyros informacija atnaujinta ir atitinka išsamią informaciją, saugomą „Dun & Bradstreet“ profilyje

Prieš pateikdami programą turite atlikti toliau nurodytus veiksmus.

- Tiksliai pateikite visą programos informaciją ir metaduomenis
- Įkelkite programos privatumo politiką ir įvykdysite skilties „Duomenų sauga“ reikalavimus
- Pateikite aktyvią demonstracinę paskyrą, prisijungimo informaciją ir visus kitus šaltinius, kurių reikia, kad „Google Play“ galėtų peržiūrėti programą (t. y. prisijungimo duomenis, QR kodą ir kt.)

Kaip visada turite užtikrinti, kad programoje būtų teikiamos stabilios, įtraukiančios, interaktyvios funkcijos naudotojams; pakartotinai patikrinti, ar visi programos elementai, įskaitant skelbimų tinklus, analitikos paslaugas ir trečiųjų šalių SDK, atitinka [„Google Play“ kūrėjų programos politiką](#); jei programos tikslinė auditorija apima vaikus, turite laikytis mūsų [šeimos politikos](#).

Siekdami garantuoti, kad programa atitinka visus reikalavimus, privalote peržiūrėti [Kūrėjų platinimo sutartį](#) ir bet kokią [Kūrėjų programos politiką](#).

Reikia daugiau pagalbos?
Išbandykite kitus toliau nurodytus veiksmus.



Susisiekite su mumis

Papasakokite daugiau ir mes jums padėsime