Norton produktu un pakalpojumu konfidencialitātes paziņojums – *pēdējoreiz atjaunināts 2019. gada 29. aprīlis*

Šis paziņojums ir jāizlasa un jāpiemēro kopā ar un papildus Symantec - Norton globālajam Paziņojumam par konfidencialitāti. Tajā ir aprakstītas Norton produktu un pakalpojumu apkopoto datu kategorijas un mērķi, saskaņā ar kuriem šīs datu kategorijas tiek apstrādātas. Tas ir paredzēts, lai sniegtu obligāto pārredzamības informāciju gan atsevišķiem Norton lietotājiem kā datu subjektiem, gan mazajiem un vidējiem uzņēmumiem, kas ir Norton lietotāji kā datu apstrādātāji. Lūdzu, ņemiet vērā, ka ar zvaigznīti atzīmētās datu kategorijas (*) ir personas dati, kas tiek nosūtīti uzņēmumam Symantec, lai nodrošinātu atbilstošās Norton produkta funkcijas un pakalpojumu funkcijas. Visas pārējās datu kategorijas tiek apkopotas Norton programmatūrā apstrādes nolūkā anonimizētā veidā.

Visi Norton Produkti un Pakalpojumi tiek turēti saskaņā ar augstākajiem standartiem, kā noteikts Symantec - Norton globālajā Paziņojumā par konfidencialitāti. Turklāt, lai pārredzami informētu jūs par katra Norton produkta un pakalpojuma unikālajām īpašībām un specifiskajiem mērķiem, papildus produkta vai pakalpojuma aprakstam šajā paziņojumā aprakstīti ievāktie Personas dati un mērķi, kuru labad Personas dati tiek apstrādāti.

Ja kāda šī Paziņojuma daļa vai aspekts jums nav pieņemams, lūdzu, nelejupielādējiet, neinstalējiet vai citādi neizmantojiet attiecīgos Produktus, Pakalpojumus vai to funkcijas, un/vai nekavējoties atinstalējiet vai pārtrauciet attiecīgo Produktu, Pakalpojumu vai funkciju izmantošanu. Attiecībā uz tiem Produktu un Pakalpojumu elementiem, kas pieprasa jums sniegt papildu Personas datus vai kas nosaka tādu Personas datu apstrādi, kas nepieciešama, lai gūtu labumu no konkrētas Produkta vai Pakalpojuma īpašas papildu funkcijas, šīs funkcijas ielādes, uzstādīšanas, aktivizēšanas vai izmantošanas laikā jums tiks lūgts pārskatīt šo Paziņojumu, lai tādējādi nodrošinātu jūsu apzinātu un atbilstošu piekrišanu.

Saturs

Norton App Lock

Produkta/pakalpojuma apraksts	Datu pieejamība un apkopošana	Datu apstrāde
Norton App Lock ļauj lietotājam nodrošināt un aizsargāt mobilās lietojumprogrammas, izmantojot atslēgu, paroli vai rakstu. Gadījumā, ja mobilā ierīce tiek nozaudēta vai nozagta, arī App Lock var konfigurēt tā, lai ierīces priekšējā kamera, ja ierīce ir attiecīgi aprīkota, pēc trim neveiksmīgiem mēģinājumiem uzņemtu attēlu un atbloķētu ierīci.	*1. Lietotāja e-pasta adrese 2. Lietotāja iestatīti PIN kodi un paroles mobilajām lietojumprogrammām 3. Pēc lietotāja izvēles attēli atkarībā no iestatījumiem	1. Lietotāja e-pasta adrese tiek iegūta un nodota Symantec, lai iespējotu Norton App Lock paroles atkopšanas un atiestatīšanas apstrādi. 2. 3. Visi citi dati, kurus produkts iegūst no lietotāja ievades, tiek saglabāti lietotāja ierīcē.

Norton Clean

Produkta/pakalpojuma apraksts	Datu pieejamība un apkopošana	Datu apstrāde
Norton Clean ir krātuves maksimizētājs, kas pārlūko lietotāja mobilās ierīces atmiņas kešatmiņu, lai izdzēstu reklāmas un nevēlamus datus un tādējādi atbrīvotu papildu atmiņu.	Mobilās ierīces unikālais ierīces identifikators (IMEI)	IMEI numurs tiek iegūts no ierīces un tiek nosūtīts uz Symantec. Pārraides laikā IMEI numurs tiek nekavējoties izmainīts pirms jebkādas papildu apstrādes. Izmaiņas tiek apstrādātas, lai uzraudzītu produkta unikālo izmantošanu. Tiklīdz dati ir izmainīti, nav iespējams izsekot sākotnējai ierīcei, lai tādējādi ne lietotājs, ne arī pati ierīce netiktu izsekota vai uzraudzīta.

Norton Error Management

Produkta/pakalpojuma apraksts	Datu pieejamība un apkopošana	Datu apstrāde
Norton Error Management dokumentu problēmas, ko nosaka Norton produkts. Šādos gadījumos lietotājs var izvēlēties paziņot Symantec par kļūdām.	1. Datora statusa informācija (sistēmas valoda, valsts valoda un operētājsistēmas versija) 2. Aktīvie procesi, to statuss un snieguma informācija 3. Dati no failiem un mapēm, kas tika atvērtas laikā, kad Norton produkts saskārās ar problēmu	1.–2.–3. Sistēmas informāciju apstrādā Symantec, lai novērstu radušos problēmu un uzlabotu Norton produkta darbību. Atsevišķos gadījumos, ja tiek konstatēta kļūda drošības apdraudējuma vai neaizsargātības dēļ, Symantec var iegūt un izplatīt konkrētus datus, kas nav saistīti ar lietotāju vai ir neatpazīstami, ar plašākas kiberbloku kopienas partneriem, piemēram, pētniecības organizācijām un citiem drošības programmatūras piegādātājiem. Šādas dalīšanas mērķis ir veicināt izpratni, atklāt un novērst risku. Symantec var izmantot statistiku, kas izgūta no informācijas, lai izsekotu un publicētu ziņojumus par drošības risku tendencēm.

Norton Community Watch

Produkta/pakalpojuma apraksts	Datu pieejamība un apkopošana	Datu apstrāde
Norton Community Watch ļauj Norton drošības produktu lietotājiem palīdzēt uzlabot identifikāciju un samazināt laiku, kas nepieciešams, lai nodrošinātu aizsardzību pret jauniem drošības draudiem. Programma apkopo atlasītos drošības un lietojumprogrammas datus un iesniedz datus Symantec analīzei, lai identificētu jaunus draudus un to avotus. Programma palīdz veidot labāku, spēcīgāku drošības produktu, analizējot lietotāja nosūtītos datus. Pievienojieties Norton Community Watch programmai: 1. Jūs palīdzat radīt labāku, spēcīgāku zināšanu loku un aizsardzību pret kiberdraudiem, izmantojot datus, kurus iesniedzat jūs pats un citi dalībnieki. Mūsu backend (aizmugures) tehnoloģija izmanto sarežģītus algoritmus, lai aprēķinātu drošības reputācijas reitingu katram failam, kas lejupielādēts, instalēts vai palaists jūsu datorā, tomēr neveicot nekādas darbības, kas būtu personīgi saistītas ar jums vai kādu citu. Norton drošības produktu lietotāji gūst priekšrocības no šīs jaunās novatoriskās tehnoloģijas, kad Norton produkts: *a. Bloķē kaitīgas lejupielādes, izmantojot Download Insight. Norton paziņo, vai jūsu lejupielāde ir atpazīstama kā droša vai nedroša vai ja tai ir nezināms drošības profils. Ja lejupielāde nav droša, mūsu produkti veic tūlītējus pasākumus, lai jūs aizsargātu; b. Nodrošina uzlabotu noteikšanas pakāpi, kā arī samazina kļūdaini pozitīvos datus; *c. Veic ātrāku skenēšanu, izmantojot Norton Insight, tādējādi ātrāk nokļūstot failos, kas tika iesniegti, analizēti un noteikti kā zināmi, izmantojot Norton Community Watch. 2. Nodrošinot kritiskos drošības un lietojumprogrammas datus, jūs nodrošināt arī izlūkdatus, kas nepieciešami, lai identificētu jaunus draudus un bloķētu tos, pirms tie nonākuši vēl tālāk. * Norton Insight ir pieejams tikai operētājsistēmā Windows OS.	1. Iekārtas ID (dati, ko ģenerē Symantec) 2. Produkta sērijas numurs (dati, kurus Symantec ir piešķīris jūsu izstrādājumam) 3. Norton konta numurs (dati, ko ģenerē Symantec) *4. Failu ceļi *5. Neizpildāmie un pārnēsājami izpildāmie faili, kas tiek identificēti kā ļaunprogrammatūra 6. To apmeklēto vietņu URL, kuras Norton produkts uzskata par potenciāli krāpnieciskām 7. Tīmekļa vietnes URL, kuru lietotājs pēdējo reizi apmeklēja pirms datora instalēšanas lejupielādes drošības riska dēļ 8. Informācija par procesiem un lietojumprogrammām, kas laiku pa laikam darbojas lietotāja ierīcē, tostarp laikā, kad rodas iespējamais drošības risks 9. Lietotāja ierīces nosūtīto datu paraugs, kas reaģē uz iespējamo drošības risku	Norton Community Watch ir pakalpojums, ko Symantec izvieto un pārvalda datu piekļuves slānī, un visi ievāktie dati tiek pārsūtīti Symantec turpmāk aprakstītājos veidos. 1. Ir nepieciešams Ierīces ID, lai izsekotu unikālo ierīču skaitu, kas izmanto produktu katram abonementam, lai pārbaudītu un pildītu licences tiesības un tiesības. 2. Katram lietotājam tiek nodrošināts produkta sērijas numurs, un to izmanto, lai nodrošinātu, ka katram produktam ir licence Symantec lietošanai. 3. Ir nepieciešams Norton Konta numurs, lai izsekotu to lietotāju skaitu, kas abonē konkrētus Norton produktus. 4.–5. Notiek failu ceļu un neizpildāmu un portatīvu izpildāmu failu iztveršana, lai palīdzētu konstatēt tādu kiberdraudu izcelsmi un loģisko atrašanās vietu, kas ietekmē lietotāja ierīci vai no tās tiek izplatīti. 6.–7. URL tiek izmantoti, lai identificētu potenciālus tīmekļa drošības risku avotus un uzlabotu Symantec produktu un pakalpojumu spēju konstatēt ļaunprātīgas darbības, kaitīgus notikumus, krāpnieciskas tīmekļa vietnes, noziedzīgus nodarījumus un citus draudus interneta drošībai. 8.–9. Ierīces dati tiek izmantoti, lai uzlabotu Symantec zināšanas un izpratni par kiberdraudiem. Ierīču dati tiek apstrādāti arī tādēļ, lai nākotnē nodrošinātu labāku aizsardzību Symantec produktu un pakalpojumu lietotājiem, kā arī kiberdrošības tendenču statistiskai analīzei.

Norton Core

Produkta/pakalpojuma apraksts	Datu pieejamība un apkopošana	Datu apstrāde
Norton Core ir bezvadu maršrutētājs, kas nodrošina aizsardzību pret ļaunprātīgu programmatūru, vīrusiem, hakeriem un citiem kiberdraudiem ierīcēm, kas ir savienotas ar maršrutētāju.	*1. Bezvadu tīkla SSID/parole (šifrēta) 2. Informācija par ierīci, ieskaitot jebkādus Personas datus, ko lietotājs ir sniedzis, piešķirot ierīces nosaukumu(–us) un, ja to nodrošina lietotājs, personas vārds vai aizstājvārds, kam ierīce ir piešķirta, un ierīces lietotāja aģenta datu/lietojumprogrammas lietotāja aģenta dati, tostarp ierīces veids, ražotājs un modelis, operētājsistēma un IP adrese 3. Dati par ierīces lietošanu, tostarp dati par pēdējās ierīces lietošanas laiku, interneta izmantošanas laiku katrai pievienotajai ierīcei un tīkla savienojumu vārtejas žurnāli 4. Vecāku kontroles informācija un iestatījumi, kā to definējuši un konfigurējuši lietotāji, tostarp bloķētās un apmeklētās tīmekļa vietnes, laika un satura filtra informācija, kā arī to tīmekļa vietņu URL, kas noteiktas vai uzskatāmas par bīstamām. *5. Personas dati, ko lietotājs var sniegt, lai izveidotu Norton kontu, tostarp lietotājvārds un papildu attēls *6. Personas dati, ko lietotājs sniedz par klientu atbalsta un savienojamības palīdzību, piemēram, lietotāja ID, vārds, loma, īpaša lietotāja politika un ierīces informācija 7. Kiberdraudu telemetrija, tostarp žurnāli par mēģinājumiem lejupielādēt ļaunprātīgus izpildāmos failus/mobilās lietojumprogrammas, citu riskantu notikumu vai darbību ieraksti un artefakti, piemēram, ļaunprātīgu programmatūru paraugi *8. Lietotāja kontaktinformācija, izteiktās vēlmes *9. Piegādes adrese un saistītā informācija 10. Norton Core nodrošina dalību Norton Community Watch	1. Bezvadu tīkla informācija tiek apstrādāta lietotāja noteiktajai Wi-Fi tīkla konfigurācijai. 2. Ierīces informācija tiek apstrādāta licences pārvaldīšanai, lai analizētu ierīci un tās datu plūsmu, lai uzraudzītu maršrutētāja veselību un savienojamību un palīdzētu to atkļūdot, lai izprastu produkta lietošanu un reaģētu uz brīdinājumiem. 3. Ierīces izmantošanas dati tiek apstrādāti šādiem mērķiem: • optimizēt Norton Core veiktspēju; • informēt lietotājus par vietnes drošību; • bloķēt pārlūkošanu nedrošās vietnēs. 4. Vecāku kontroles informācija un iestatījumi tiek izmantoti, lai pildītu noteikumus un politiku, kuru lietotājs noteicis saviem pārvaldītajiem profiliem, palīdzētu lietotājam atklāt jebkādu ar šādiem profiliem saistītu Personas datu ļaunprātīgu izmantošanu un sazinātos ar lietotāju un pārvaldītajiem profiliem. 5.–6. Lietotāja konta informāciju Symantec apkopo, lai izpildītu klienta līgumā norādītos pakalpojumus un sniegtu tehnisko atbalstu un palīdzību. 7. Lai veiktu pētījumus un izstrādi, lai uzlabotu Symantec produktus un pakalpojumus, kā arī labāk aizsargātu lietotāja tīklu, ierīces, datus un identitāti, Symantec pārraida koberdraudu telemetriju. 8. Lietotāja kontaktinformācija un preferences tiek pārsūtītas Symantec šādiem nolūkiem: • Norton Core programmatūras instalēšanas procesa vadīšanai lietotājam; • lietotāja pieredzes uzlabošanas paņēmienu paziņošanai lietotājam; • lietotājam sniegtās informācijas pielāgošanai, pamatojoties uz lietotāja vēlmēm (piemēram, valodu un ģeogrāfisko reģionu); • klienta apmierinātības uzlabošanai par sniegtajiem pakalpojumiem, izmantojot īpašos un trešo personu zvanu centrus. 9. Piegādes adrese un saistītā informācija tiek apstrādāta, lai lietotājam piegādātu Norton Core aparatūru. 10. Attiecībā uz informāciju par Norton Community Watch, lūdzu, skatiet sīkāku informāciju šī paziņojuma sadaļā Norton Community Watch. Turklāt Symantec izmantos apkopotus, neidentificējamus, anonimizētus vai citādi neidentificētus datus, kas iegūti no ievāktiem datiem, piemēram, statistikas: • vispārēju kiberdrošības pētījumu veikšanai; • ļaunprogrammatūras un kiberdraudu atklāšanas uzlabošanai, piemēram, izmantojot failu paraugu analīzi; • ziņojumu par drošības un identitātes zādzības riskiem/tendencēm izsekošanai un publicēšanai; • produktu izvietošanas statistiskās analīzes veikšanai, tostarp tendenču un salīdzinājumu analīzei mūsu apvienotajā lietotāju bāzē; • produkta veiktspējas uzraudzībai un uzlabošanai attiecībā uz pieejamību un reakcijas laiku; • lai izprastu ar produktiem saistītu saziņas biežumu, lai optimizētu vispārējo lietotāju pieredzi; un

		• iegūtu citu, ar lietotāju nesaistītu, uzņēmējdarbības un tirgus ieskatu, kas ir būtisks, lai uzlabotu mūsu darbību.

Norton Mobile Security

Produkta/pakalpojuma apraksts	Datu pieejamība un apkopošana	Datu apstrāde
Norton Mobile Security aizsargātajiem lietotājiem un to ierīcēm, kuras abonents izvēlas aizsargāt, nodrošina viedtālruņu un planšetdatoru aizsardzību pret digitālajiem draudiem, pazaudētas vai nozagtas ierīces atgūšanu un kontaktinformācijas atjaunošanu	1. Aizsargāto lietotāju mobilo ierīču dati, tostarp aprīkojuma identifikatori (piemēram, IMEI, WiFi MAC adrese, UDID), abonenta informācija, mobilā tālruņa numurs un cita aizsargāta lietotāja kontaktinformācija, ierīces nosaukums/veids un ražotājs, operētājsistēmas veids un versija, bezvadu pārvadātājs, tīkla veids, izcelsmes valsts, atbalsta lietas ID, lietotāja instalētie sertifikāti, vietnes domēna vārds un saistītā SSL sertifikātu ķēde no ierīces un IP adrese 2. Lietojuma dati, piemēram, informācija par lejupielādēm un izmantošanas biežumu, žurnāla dati un sīkdatnes, kā arī tīkla pakalpojumu informācija par to, kā lietotājs pieslēdzas tīkla pakalpojumiem 3. Failu un lietojumprogrammu nosaukumi lietotāja ierīcē katru reizi, kad Produkts veic skenēšanu, tostarp skenētās lietotnes, kuras pašlaik nav Symantec zināmo lietotņu datubāzē, lai aizsargātu lietotāju pret ļaunprogrammatūru vai riskantajām funkcijām, kā arī Kalendāra un SD karšu saturs, ja tas ir pieejams 4. Tīmekļa pārlūkošanas URL, vēsture un grāmatzīmes *5. Pēc lietotāja izvēles — kontakti lietotāja ierīcē, tostarp zvanu un SMS žurnāli 6. Tālruņa zvanu un ierīces audio iestatījumi	1. Mobilo ierīču dati, abonenta informācija un aizsargātā lietotāja kontaktinformācija tiek apstrādāta, lai: • iespējotu produkta veiktspēju un optimizēšanu; • autentificētu Symantec aizsargātā lietotāja identitāti; • vadītu lietotāju programmatūras instalēšanas procesa laikā; • sazinātos ar aizsargāto lietotāju pakalpojuma sniegšanai; • licences pārvaldīšanai; un • klienta apmierinātības uzlabošanai par sniegtajiem pakalpojumiem, izmantojot īpašos un trešo personu zvanu centrus. 2. Lietojuma dati tiek apstrādāti šādiem mērķiem: izpratnei par produkta lietošanu un preferencēm, lai personalizētu un uzlabotu lietotāju pieredzi. 3. Failu, lietojumprogrammu nosaukumi, kalendārs (piemēram, URL ielūgumos) un SD kartes saturs tiek apstrādāts, lai: • brīdinātu lietotāju par potenciāli kaitīgām lietojumprogrammām; • veiktu ierīces skenēšanu, meklējot ļaunprātīgas programmas; • no ierīces noslaucītu personīgo saturu, ja lietotājs izvēlas aktivizēt un izpildīt produkta Wipe (Noslaucīt) komandu. 4. Pārlūkošanas dati tiek apstrādāti šādiem mērķiem: • informēt lietotājus par vietnes drošību; • bloķēt pārlūkošanu nedrošās vietnēs; • noslaucīt pārlūkošanas vēsturi un grāmatzīmes, ja lietotājs izvēlas izmantot produkta Web Protection (Tīkla aizsardzība) funkciju vai komandu Wipe (Slaucīt). 5. Kontaktpersonas, tostarp zvanu un SMS žurnāli lietotāja ierīcē, tiek apstrādāti, lai nodrošinātu zvanu/īsziņu bloķēšanas funkcijas, ja lietotājs izvēlas tās izmantot. 6. Tālruņa iestatījumi tiek izmantoti, lai bloķētu ienākošos zvanus no kontaktiem vai modificētu ierīces audio iestatījumus, ja lietotājs izvēlas iespējot un izmantot Produkta bloķēšanas funkciju un/vai komandu Scream (Kliedziens). 7. 8. Ierīces atrašanās vietu un attēla datus var apkopot pēc aizsargātā lietotāja pieprasījuma, lai noteiktu lietotāja ierīces atrašanās vietu, kad tā tiek nozaudēta vai nozagta. Produkts var arī nodrošināt abonentam tālvadības komandas, lai palīdzētu atrast aizsargāto lietotāja ierīci, ja tā tiek nozaudēta vai nozagta. Dažos gadījumos, kad tiek ziņots par nozaudētu vai nozagtu ierīci, tā no attāluma tiks bloķēta. Turpretī, kad tiek ziņots par nozaudētu vai nozagtu ierīci, produktu var arī jebkurā laikā slēgt. Ar aizsargātā lietotāja atļauju var tikt saglabāta vēsture par to, kuras ir pēdējās desmit atrašanās vietas, kur ierīce bijusi, lai aizsargātais lietotājs varētu izsekot ierīces pēdējām kustībām, pat ja produkts pašlaik netiek izmantots.

	*7. Ierīces atrašanās vietas dati *8. Produktu var arī konfigurēt tā, lai ierīces priekšējā kamera uzņem attēlu tad, kad ierīce tiek izmantota, kad tiek ievadīta nepareiza parole pēc viena neveiksmīga mēģinājuma ierīci atbloķēt vai kad ierīce tiek ieslēgta pēc tam, kad tā bijusi izslēgta 9. Mobilajā ierīcē esošo datu dublējumkopija, tostarp kontakti, zvanu vēsture, tālruņa numuri un īsziņas	9. Dublēšanas dati tiek apstrādāti, lai piegādātu produkta dublējuma un atkopšanas funkcijas, ja lietotājs izvēlas tās izmantot. Turklāt Symantec izmantos apkopotus, neidentificējamus, anonimizētus vai citādi neidentificētus datus, kas iegūti no ievāktiem datiem, piemēram, statistikas: • vispārēju kiberdrošības pētījumu veikšanai; • ļaunprogrammatūras un kiberdraudu atklāšanas uzlabošanai, piemēram, izmantojot failu paraugu analīzi; • ziņojumu par drošības un identitātes zādzības riskiem/tendencēm izsekošanai un publicēšanai; • produktu izvietošanas statistiskās analīzes veikšanai, tostarp tendenču un salīdzinājumu analīzei mūsu apvienotajā lietotāju bāzē; • produkta veiktspējas uzraudzībai un uzlabošanai attiecībā uz pieejamību un reakcijas laiku; • lai izprastu ar produktiem saistītu saziņas biežumu, lai optimizētu vispārējo lietotāju pieredzi; un • iegūtu citu, ar lietotāju nesaistītu, uzņēmējdarbības un tirgus ieskatu, kas ir būtisks, lai uzlabotu mūsu darbību.

Norton Security Scan

Produkta/pakalpojuma apraksts	**Datu pieejamība un apkopošana**	**Datu apstrāde**
Norton Secure Scan nodrošina lietotāja izvēlētās gala ierīces vai ierīču skenēšanu, identificē potenciālās problēmas vai riskus, kā arī iesaka lietotājam produktus un risinājumus.	1. Ierīces ID (dati, ko Symantec izveidojis iekšēji); ierīces instalēšana/atinstalēšana; informācija par ierīci un ierīces lietotāja aģentu dati/lietotņu lietotāju aģentu dati, tostarp ierīces veids, OS versija, OS valoda, ražotājs un modelis; operētājsistēma; saistītā ģeogrāfiskā informācija 2. Telemetrijas informācija par skenētajiem failiem, lietotāju pieredzi un konstatētajiem, novērstajiem un atlikušajiem draudiem; datums un laiks pēc skenējuma iesniegšanas; informācija par instalēšanas un darbību statusu, kas var nejauši ietvert personas datus, ja tie atrodas faila ceļā vai mapes nosaukumā	1. Ierīces ID un ar to saistīto informāciju Symantec izmanto, lai: • vadītu lietotāju programmatūras instalēšanas procesa laikā; • saziņai ar lietotāju, lai nodrošinātu pakalpojumu; • izpratnei par pakalpojuma lietošanu un preferencēm, lai personalizētu un uzlabotu lietotāju pieredzi. 2. Telemetrijas informāciju Symantec izmanto šādiem mērķiem: • Pakalpojumu iespējošanai un optimizēšanai; un • pētniecībai un izstrādei, lai uzlabotu Symantec produktus un pakalpojumus un labāk aizsargātu lietotāja tīklu, ierīces, datus un identitāti. Turklāt Symantec izmantos apkopotus, neidentificējamus, anonimizētus vai citādi neidentificētus datus, kas iegūti no ievāktiem datiem, piemēram, statistikas: • vispārēju kiberdrošības pētījumu veikšanai; • ļaunprogrammatūras un kiberdraudu atklāšanas uzlabošanai, piemēram, izmantojot failu paraugu analīzi; • ziņojumu par drošības un identitātes zādzības riskiem/tendencēm izsekošanai un publicēšanai; • produktu izvietošanas statistiskās analīzes veikšanai, tostarp tendenču un salīdzinājumu analīzei mūsu apvienotajā lietotāju bāzē; • produkta veiktspējas uzraudzībai un uzlabošanai attiecībā uz pieejamību un reakcijas laiku; • lai izprastu ar produktiem saistītu saziņas biežumu, lai optimizētu vispārējo lietotāju pieredzi; un • iegūtu citu, ar lietotāju nesaistītu, uzņēmējdarbības un tirgus ieskatu, kas ir būtisks, lai uzlabotu mūsu darbību.

Norton Secure Login

Produkta/pakalpojuma apraksts	Datu pieejamība un apkopošana	Datu apstrāde
Norton Secure Login (NSL) ir identitātes nodrošinātājs, kas nodrošina vienkāršu, drošu un centralizētu lietotāju autentificēšanu. Symantec nodrošina identitātes pārvaldības infrastruktūru miljoniem lietotāju dažādos Norton produktos.	*1. Personas dati, lai autentificētu lietotāja identitāti, piemēram, mājas adrese, tālruņa numurs, dzimšanas datums un/vai kredītkartes numurs; lietotāja kontaktinformācija; jebkādi papildu personas dati, ko lietotājs var ievadīt Norton lietotāja kontā vai ko lietotājs var sniegt klientu atbalsta un savienojuma palīdzības nolūkos, piemēram, vārds un informācija par ierīci 2. Informācija par ierīci, produktu un pakalpojumu un ierīces lietotāja aģenta dati/lietotnes lietotāja aģenta dati, tostarp ierīces veids; ražotājs; modelis; operētājsistēma un versija; informācija par ierīci un ierīces lietotāja aģenta dati/lietotnes lietotāja aģenta dati, tostarp ierīces veids; ražotājs; modelis; operētājsistēma un versija; izpildlaika dati; instalētās lietojumprogrammas; saistītā ģeogrāfiskā informācija, MAC adrese un IP adrese 3. Lietošanas dati par interneta lietošanu, piemēram, tīmekļa vietņu URL un apmeklēto tīmekļa vietņu IP adreses, meklēšanas atslēgvārdi un rezultāti, kā arī informācija par potenciālajiem drošības riskiem (tostarp to tīmekļa vietņu URL un IP adreses, kuras uzskatāmas par potenciāli krāpnieciskām un kurās var būt personas dati, kurus tīmekļa vietne mēģina iegūt bez lietotāja atļaujas)	1. Personas datus Symantec apstrādā šādiem mērķiem: • autentificēt lietotāja identitāti Symantec vai uzticamām trešajām pusēm, kas izmanto Norton Security Login lietotājvārdu; • izsniegt identitātes sertifikātu un/vai izvairīties no krāpnieciskiem darījumiem lietotāja vārdā; • vadīt lietotāju iestatīšanas procesa laikā; • saziņai ar lietotāju, lai nodrošinātu pakalpojumu, tostarp atbalstu un palīdzību; un • klienta apmierinātības uzlabošanai par sniegtajiem pakalpojumiem, izmantojot īpašos un trešo personu zvanu centrus. 2. Informāciju par ierīci, produktu un pakalpojumu Symantec apstrādā šādiem mērķiem: • Pakalpojumu un Produktu snieguma iespējošanai un optimizēšanai; • licences pārvaldīšanai; un • izpratnei par produkta lietošanu un preferencēm, lai personalizētu un uzlabotu lietotāju pieredzi. 3. Lietošanas datus Symantec apstrādā šādiem mērķiem: • informēt lietotājus par vietnes drošību; • bloķēt pārlūkošanu nedrošās vietnēs; • pētniecībai un izstrādei, lai uzlabotu Symantec produktus un pakalpojumus un labāk aizsargātu lietotāja tīklu, ierīces, datus un identitāti. Turklāt Symantec izmantos apkopotus, neidentificējamus, anonimizētus vai citādi neidentificētus datus, kas iegūti no ievāktiem datiem, piemēram, statistikas: • vispārēju kiberdrošības pētījumu veikšanai; • ļaunprogrammatūras un kiberdraudu atklāšanas uzlabošanai, piemēram, izmantojot failu paraugu analīzi; • ziņojumu par drošības un identitātes zādzības riskiem/tendencēm izsekošanai un publicēšanai; • produktu izvietošanas statistiskās analīzes veikšanai, tostarp tendenču un salīdzinājumu analīzei mūsu apvienotajā lietotāju bāzē; • produkta veiktspējas uzraudzībai un uzlabošanai attiecībā uz pieejamību un reakcijas laiku; • lai izprastu ar produktiem saistītu saziņas biežumu, lai optimizētu vispārējo lietotāju pieredzi; un • iegūtu citu, ar lietotāju nesaistītu, uzņēmējdarbības un tirgus ieskatu, kas ir būtisks, lai uzlabotu mūsu darbību.

Norton Ultimate palīdzības dienests un Norton Computer Tune-Up

Produkta/pakalpojuma apraksts	**Datu pieejamība un apkopošana**	**Datu apstrāde**
Norton Ultimate palīdzības dienests ļauj lietotājam sazināties ar ekspertu, lai palīdzētu tehniskos jautājumos, sākot no tīkla iestatīšanas līdz ierīču diagnostikai un problēmu novēršanai. Norton Computer Tune-Up ir funkcija Norton Ultimate palīdzības dienestā, kas palīdz lietotāja ierīci saglabāt kā jaunu, izmantojot diagnostiku.	*1. Informācija par pieprasījumu, kuru jūs sniedzat Symantec pakalpojumu pārstāvjiem pa tālruni vai kuru ievadāt Symantec tiešsaistes saskarnē, pieprasot Norton pakalpojumus 2. Informācija par sistēmu, tostarp: jūsu ierīcē izmantotās operētājsistēmas un pārlūkprogrammas veids un versija; vai ir aktīvs ugunsmūris; vai ir instalēta pretvīrusu programmatūra, vai tā darbojas un ir atjaunināta; atmiņas un diska vieta, starpniekservera konfigurācija un direktoriju saraksti atbalsta programmatūras rīkā; informācija par pārlūkprogrammu, tostarp drošības un pagaidu failu iestatījumi; ierīces aktīvie porti, mitināšanas faili un tīkla saskarnes iestatījumi; informācija par instalētajām programmām un aktīvajiem procesiem; informācija no lietotnes un operētājsistēmas žurnāla failiem un reģistra datiem 3. Informācija par diagnostiku, tostarp: skenēto failu skaits, atbalsta programmatūras rīka atklātie un novērstie draudi; atklāto draudu veidi; ierīces drošības stāvoklis (labs/normāls/slikts), kā noteikts ar atbalsta programmatūras rīku; to atlikušo draudu skaits un veids, kurus atbalsta programmatūras rīks nav novērsis	1. Pieprasīto informāciju Symantec apstrādā šādiem mērķiem: • saziņai ar lietotāju, lai nodrošinātu pakalpojumu; • izpratnei par produkta lietošanu un preferencēm, lai personalizētu un uzlabotu lietotāju pieredzi; un • klienta apmierinātības uzlabošanai par sniegtajiem pakalpojumiem, izmantojot īpašos un trešo personu zvanu centrus. 2. Sistēmas informāciju Symantec apstrādā šādiem mērķiem: • lietotāja pieprasīto pakalpojumu nodrošināšanai; • pakalpojumu iespējošanai un optimizēšanai; un • lietotāja vadīšanai Pakalpojumu izmantošanas laikā; 3. Diagnostikas informāciju Symantec apstrādā šādiem mērķiem: • lai informētu lietotāju par sniegto pakalpojumu iznākumu; un • pētniecībai un izstrādei, lai uzlabotu Symantec produktus un pakalpojumus un labāk aizsargātu lietotāja tīklu, ierīces, datus un identitāti. Turklāt Symantec izmantos apkopotus, neidentificējamus, anonimizētus vai citādi neidentificētus datus, kas iegūti no ievāktiem datiem, piemēram, statistikas: • vispārēju kiberdrošības pētījumu veikšanai; • ļaunprogrammatūras un kiberdraudu atklāšanas uzlabošanai, piemēram, izmantojot failu paraugu analīzi; • ziņojumu par drošības un identitātes zādzības riskiem/tendencēm izsekošanai un publicēšanai; • produktu izvietošanas statistiskās analīzes veikšanai, tostarp tendenču un salīdzinājumu analīzei mūsu apvienotajā lietotāju bāzē; • produkta veiktspējas uzraudzībai un uzlabošanai attiecībā uz pieejamību un reakcijas laiku; • lai izprastu ar produktiem saistītu saziņas biežumu, lai optimizētu vispārējo lietotāju pieredzi; un • iegūtu citu, ar lietotāju nesaistītu, uzņēmējdarbības un tirgus ieskatu, kas ir būtisks, lai uzlabotu mūsu darbību.

Norton Secure VPN (agrāk Norton WiFi Privacy)

Produkta/pakalpojuma apraksts	Datu pieejamība un apkopošana	Datu apstrāde
Norton Secure VPN aizsargā lietotāja ierīces un lietotāja datus, šifrējot lietotāja informāciju par jebkuru interneta pieslēgumu un saglabājot lietotāja privātumu.	1. Abonenta informācija un mobilās ierīces dati, tostarp ierīces nosaukums, tips, operētājsistēmas versija un valoda. 2. Kopējais joslas platuma lietojums. 3. Pagaidu lietošanas dati, lai palīdzētu novērst problēmas ar pakalpojumu.	1. Abonenta informāciju un mobilā ierīces datus Symantec apstrādā šādiem mērķiem: • pakalpojumu snieguma iespējošanai un optimizēšanai; • izpratnei par produkta lietošanu un preferencēm, lai personalizētu un uzlabotu lietotāju pieredzi; • lietotāja vadīšanai programmatūras instalēšanas un pakalpojuma izmantošanas laikā; • saziņai ar lietotāju, lai nodrošinātu pakalpojumu; • atgādinātu lietotājam aizsargāt informāciju, ko lietotājs nosūta; un • klienta apmierinātības uzlabošanai par sniegtajiem pakalpojumiem, izmantojot īpašos un trešo personu zvanu centrus. 2. Joslas platuma lietojuma datus Symantec apstrādā norēķinu, tīkla darbību un atbalsta mērķiem. 3. Pagaidu lietošanas datus Symantec apstrādā šādiem mērķiem: • vispiemērotākā savienojuma servera izvēle; un • pētniecībai un izstrādei, lai uzlabotu Symantec produktus un pakalpojumus un labāk aizsargātu lietotāja tīklu, ierīces, datus un identitāti. Izmantojot Norton Secure VPN, mēs maršrutējam lietotāja interneta datplūsmu, izmantojot Symantec tīklu, kas ir “No Log” tīkls. Tas nozīmē, ka, pieslēdzoties Norton Secure VPN, Symantec neuzglabā lietotāja izcelsmes IP adresi, tādēļ Symantec nevar identificēt personas. Symantec automatizētā noteikumu bāzētā satiksmes vadība var prasīt datu plūsmu internetā reāllaika analīzē, tostarp galamērķa tīmekļa vietnēs vai IP adresēs un izcelsmes IP adresēs, lai gan netiek uzturēts žurnāls attiecībā uz šo informāciju. Symantec neuzglabā informāciju par lietojumprogrammatūrām, pakalpojumiem vai tīmekļa vietnēm, kuras lietotājs lejupielādē, izmanto vai apmeklē. Tā kā Symantec pārvalda globālo tīklu, lietotāja interneta datplūsmu var novirzīt pa vienu vai vairākām dažādām valstīm, kā paskaidrots Symantec - Norton Global paziņojumā par privātumu. Turklāt Symantec izmantos apkopotus, neidentificējamus, anonimizētus vai citādi neidentificētus datus, kas iegūti no ievāktiem datiem, piemēram, statistikas: • vispārēju kiberdrošības pētījumu veikšanai; • ļaunprogrammatūras un kiberdraudu atklāšanas uzlabošanai, piemēram, izmantojot failu paraugu analīzi; • ziņojumu par drošības un identitātes zādzības riskiem/tendencēm izsekošanai un publicēšanai; • produktu izvietošanas statistiskās analīzes veikšanai, tostarp tendenču un salīdzinājumu analīzei mūsu apvienotajā lietotāju bāzē; • produkta veiktspējas uzraudzībai un uzlabošanai attiecībā uz pieejamību un reakcijas laiku; • lai izprastu ar produktiem saistītu saziņas biežumu, lai optimizētu vispārējo lietotāju pieredzi; un • iegūtu citu, ar lietotāju nesaistītu, uzņēmējdarbības un tirgus ieskatu, kas ir būtisks, lai uzlabotu mūsu darbību.

Norton Security produkti (Security, Internet Security, One, Antivirus & 360)

Šajā sadaļā aprakstītas Norton Security (Standard, Deluxe un Premium), Norton Internet Security, Norton One, Norton Antivirus, Norton Antivirus Basic, Norton 360, Norton 360PE un Norton 360MD.

Produkta/pakalpojuma apraksts	**Datu pieejamība un apkopošana**	**Datu apstrāde**
Norton Security produkti nodrošina galapunktu drošību, kas aizsargā pret izspiedējprogrammatūru, vīrusiem, spiegprogrammatūru, ļaunprogrammatūru un citiem tiešsaistes draudiem.	1. Abonenta informācija un ierīces dati, tostarp *Personas dati, kurus lietotājs var ievadīt, lai izveidotu Norton kontu, piemēram, lietotājvārds un papildu attēls; jebkuri *Personas dati, kurus lietotājs iekļauj, piešķirot ierīces nosaukumu (-us) un, ja tas ir norādīts, tās personas vārdu vai aizstājvārdu, kurai ierīce ir piešķirta, un ierīces lietotāja aģenta datu/lietotnes lietotāja aģenta dati, tostarp ierīces veids, ražotājs un modelis; operētājsistēma un versija; lietojumprogrammas un versijas; saistītā ģeogrāfiskā informācija, MAC adrese, ierīces ID un IP adrese; Statusa informācija par uzstādīšanu un darbību, kas var nejauši ietvert Personas datus, ja tie minēti failā vai mapes nosaukumā; jebkuri papildu Personas dati, kurus lietotājs sniedz Symantec klientu atbalsta centram un savienojamības atbalstam, piemēram, lietotāja ID, nosaukums, loma, politikas un ierīces informācija 2. Dati par interneta lietošanu, piemēram, tīmekļa vietņu URL un apmeklēto tīmekļa vietņu IP adreses, meklēšanas atslēgvārdi un rezultāti, kā arī informācija par potenciālajiem drošības riskiem (tostarp to tīmekļa vietņu URL un IP adreses, kuras uzskatāmas par potenciāli krāpnieciskām un kurās var būt personas dati, kurus tīmekļa vietne mēģina iegūt bez lietotāja atļaujas) 3. Dati par ierīces lietošanu un diagnostiku, tostarp: dati par pēdējās ierīces lietošanas laiku, katras pievienotās ierīces interneta izmantošanas laiku un vārtejas žurnāls, kas sīki apraksta tīkla savienojuma darbības; izpildāmie faili, kas identificēti kā potenciāli ļaunprogrammatūras, kas var ietvert Personas datus, ko iegūst ļaunprogrammatūra bez lietotāja atļaujas; Symantec sūtītie E-pasta ziņojumiem, kuri ar lietotāja atļauju reģistrēti kā mēstules, vai nepareizi identificēti kā mēstules; informācija par “Crash dump” vai pārskatā iekļauto informāciju, kuru lietotājs var nosūtīt Symantec, kad produkti un pakalpojumi saskaras ar problēmu, kas kļūdas rašanās laikā var būt sistēmas valoda, valsts valoda, operētājsistēma un darbojošies procesi/atvērtie faili 4. Vecāku kontroles informācija un iestatījumi, kā to definējuši un konfigurējuši lietotāji, tostarp bloķētās un apmeklētās tīmekļa vietnes, laika un satura filtra informācija, kā arī to tīmekļa vietņu URL, kas noteiktas vai uzskatāmas par bīstamām.	1. Abonenta informāciju un ierīces datus Symantec apstrādā šādiem mērķiem: • Produktu un Pakalpojumu snieguma iespējošana un optimizēšanai; • autentificētu Symantec aizsargātā lietotāja identitāti; • izpratnei par produkta lietošanu un preferencēm, lai personalizētu un uzlabotu lietotāju pieredzi; • vadītu lietotāju programmatūras instalēšanas procesa laikā; • saziņai ar lietotāju, lai nodrošinātu pakalpojumu; • licences pārvaldīšanai; un • klienta apmierinātības uzlabošanai par sniegtajiem pakalpojumiem, izmantojot īpašos un trešo personu zvanu centrus. 2. Dati par interneta lietojumu tiek apstrādāti šādiem mērķiem: • informēt lietotājus par vietnes drošību; • bloķēt pārlūkošanu nedrošās vietnēs. 3. Datus par ierīces lietojumu un diagnostiku Symantec apstrādā šādiem mērķiem: • izpratnei par produkta lietošanu; • Produktu un Pakalpojumu aizsardzības līdzekļu nodrošināšanai; • pētniecībai un izstrādei, lai uzlabotu Symantec produktus un pakalpojumus un labāk aizsargātu lietotāja tīklu, ierīces, datus un identitāti. 4. Vecāku kontroles informācija un iestatījumi tiek izmantoti, lai liktu ievērot lietotāja definētās kārtulas un politikas, kuras lietotājs ir noteicis saviem kontrolētajiem profiliem, palīdzētu lietotājam konstatēt savu Personas datu nepareizu lietošanu saistībā ar šādiem profiliem un lai sazinātos ar lietotāju un kontrolētajiem profiliem. Turklāt Symantec izmantos apkopotus, neidentificējamus, anonimizētus vai citādi neidentificētus datus, kas iegūti no ievāktiem datiem, piemēram, statistikas: • vispārēju kiberdrošības pētījumu veikšanai; • ļaunprogrammatūras un kiberdraudu atklāšanas uzlabošanai, piemēram, izmantojot failu paraugu analīzi; • ziņojumu par drošības un identitātes zādzības riskiem/tendencēm izsekošanai un publicēšanai; • produktu izvietošanas statistiskās analīzes veikšanai, tostarp tendenču un salīdzinājumu analīzei mūsu apvienotajā lietotāju bāzē; • produkta veiktspējas uzraudzībai un uzlabošanai attiecībā uz pieejamību un reakcijas laiku; • lai izprastu ar produktiem saistītu saziņas biežumu, lai optimizētu vispārējo lietotāju pieredzi; un • iegūtu citu, ar lietotāju nesaistītu, uzņēmējdarbības un tirgus ieskatu, kas ir būtisks, lai uzlabotu mūsu darbību.

Norton Safe Search, Norton Home Page, Norton Safe Web

Produkta/Pakalpojuma apraksts	Datu pieejamība un apkopošana	Datu apstrāde
Norton Safe Search ir meklētājprogrammas tīmekļa vietne, kas palīdz aizsargāt lietotāju no nedrošām tīmekļa vietnēm, filtrējot meklēšanas rezultātus un lietotājam rādot vietņu drošības novērtējumus, tādējādi piedāvājot drošāku tīmekļa pārlūkošanu. Tā ir arī pārlūkprogrammas paplašinājums, kas dažādos veidos nodrošina piekļuvi Norton Safe Search tīmekļa vietnei. Dažādas šī paplašinājuma versijas pēc lietotāja izvēles var: a) pārlūkprogrammas noklusējuma meklētājprogrammas vietā izmantot Norton Safe Search tīmekļa vietni; vai b) pārlūkprogrammas noklusējuma meklētājprogrammas iestatījuma vietā izmantot Norton Safe Search tīmekļa vietni UN pārlūkprogrammas noklusējuma sākumlapas vietā + jaunas cilnes iestatījumu vietā izmantot Norton Home Page. Norton Home Page ir pārlūkprogrammas paplašinājums un noklusējuma sākumlapa, kas iespējo Norton Safe Search tīmekļa vietni. Norton Safe Web ir pārlūkprogrammas paplašinājums, kuru lietotājs izvēlas, lai uzraudzītu pārlūkošanas aktivitāti un tīmekļa lapu saturu. Lai palīdzētu aizsargāt lietotāju pret ļaunprātīgu vietņu saturu, pikšķerēšanu un citiem apdraudējumiem, tas izmanto reputācijas pakalpojumus un tīmekļa lapu satura analīzi.	1. Abonenta informācija un ierīces un programmatūras dati, tostarp: tīmekļa pārlūkprogrammas nosaukums, versija un vēlamā valoda; operētājsistēma, versija vai platforma; lietotāja ierīces IP adrese 2. Pakalpojuma lietojuma dati, tostarp: saites sociālajā medijā un tīmekļa e-pastā; tīmekļa vietņu pārlūkošanas aktivitāte; tīmeklī meklētie vārdi; noklusējuma ievades dažādos meklēšanas lodziņos, kurus pārvalda Norton produkti; meklētājprogrammas rezultāti 3. Sīkfaili, pikseļu tagi, skripti vai līdzīgas tehnoloģijas, kuras datorā vai ierīcē ievieto Norton Safe Search tīmekļa vietne un Norton Home Page tīmekļa vietne	1. Abonementa informāciju un ierīces un programmatūras datus Symantec apstrādā tālāk šādiem mērķiem: • pakalpojumu snieguma iespējošanai un optimizēšanai; • licences pārvaldīšanai; • izpratnei par produkta lietošanu un preferencēm, lai personalizētu un uzlabotu lietotāju pieredzi; • vadītu lietotāju programmatūras instalēšanas procesa laikā; • Produktu un Pakalpojumu uzlabojumu sniegšanai, lai labāk aizsargātu lietotāju, lietotāja tīklu, ierīci, datus un identitāti; • klienta apmierinātības uzlabošanai par sniegtajiem pakalpojumiem, izmantojot īpašos un trešo personu zvanu centrus. 2. Pakalpojumu lietojuma datus apstrādā Symantec, un šie dati tiek apstrādāti Symantec vārdā šādiem mērķiem: • informēt lietotājus par vietnes drošību; • bloķēt pārlūkošanu nedrošās vietnēs; • pakalpojuma lietojuma analizēšanai. Lietotāja meklēšanas vaicājumu pieprasījumi, kas tiek veikti caur mūsu Norton Safe Search produktu, tiek novirzīti uz mūsu Trešo pušu meklēšanas partneriem Oath/Yahoo! (ASV un Kanādai) un IACI (ārpus ASV/Kanādas), lai jums nodrošinātu vaicājuma izpēti. Mūsu Trešo pušu partneriem ir arī tiesības vākt informāciju tieši no jums saistībā ar jūsu darbībām pakalpojumā Norton Safe Search. Mūsu Trešo pušu partneri šos datus vāc kā datu pārziņi, ar mērķi apstrādāt jūsu meklēšanas vaicājumu. Šādu datu vākšanuregulē Trešo pušu partneru Konfidencialitātes politika, Deklarācija un Paziņojums. Lai jums nodrošinātu Norton Safe Search pakalpojumu, jūsu meklēšanas vaicājuma pieprasījums tiek novirzīts mūsu Trešās puses partnerim (t.i., tas netiek novirzīts Symantec uzņēmumam), kur šis Trešās puses partneris apstrādā jūsu pieprasījumu. Trešās puses partnerim ir arī tiesības vākt informāciju tieši no jums saistībā ar jūsu darbībām pakalpojumā Norton Safe Search (šī informācija kopā tiek saukta par “Trešo pušu datiem”). Jūsu meklēšanas vaicājuma apstrādāšanas nolūkos Trešās puses partneris ir datu pārzinis, tādēļ tieši mūsu Trešās puses partneris, nevis Symantec, izlemj veidu, kā tiek vākti, izmantoti, izpausti, paturēti vai kā citādi apstrādāti jūsu Trešo pušu dati. Uz jūsu Trešo pušu datiem attiecas Trešās puses partnera paziņojumi par konfidencialitāti, kas regulē jūsu datu apstrādāšanu meklēšanas vaicājuma izpildes nolūkos. Lūdzu, skatiet mūsu Trešās puses partnera paziņojumus par konfidencialitāti. 3. Sīkfaili un līdzīgi indeksētāji tiek apstrādāti tālāk norādīto līdzekļu lietošanas preferenču un vēstures nolūkos. Papildinformāciju par sīkfailiem, lūdzu, skatiet iepriekšējā sadaļā ar nosaukumu “Izsekošanas tehnoloģijas, sīkfaili un norādījums par neizsekošanu”, dokumentā Symantec — Norton globālais paziņojums par konfidencialitāti. Kritisko kļūdu statistiskās analīzes un pārvaldības nolūkos ar Google Analytics mērījumu protokolu tiek apstrādātas anonimizētas IP adreses un informācija par produktu lietojumu. Noklikšķiniet šeit, lai iegūtu informāciju par Google Analytics datu aizsardzību. Turklāt Symantec izmantos apkopotus, neidentificējamus, anonimizētus vai citādi neidentificētus datus, kas iegūti no ievāktiem datiem, piemēram, statistikas: • vispārēju kiberdrošības pētījumu veikšanai; • ļaunprogrammatūras un kiberdraudu atklāšanas uzlabošanai, piemēram, izmantojot failu paraugu analīzi; • ziņojumu par drošības un identitātes zādzības riskiem/tendencēm izsekošanai un publicēšanai; • produktu izvietošanas statistiskās analīzes veikšanai, tostarp tendenču un salīdzinājumu analīzei mūsu apvienotajā lietotāju bāzē; un • Produkta veiktspējas uzraudzībai un uzlabošanai attiecībā uz pieejamību un reakcijas laiku.

Norton Security Toolbar

Produkta/Pakalpojuma apraksts	Datu pieejamība un apkopošana	Datu apstrāde
Rīkjoslai Norton Security Toolbar ir divi varianti — a) pievienojumprogramma pārlūkprogrammai Microsoft Internet Explorer; un b) pārlūkprogrammas Google Chrome paplašinājums. Abus variantus lietotājs izmanto, lai pārraudzītu lietotāja pārlūkošanas aktivitātes un tīmekļa lapu saturu. Lai palīdzētu lietotāju aizsargāt pret ļaunprātīgu tīmekļa vietņu saturu, pikšķerēšanu un citiem apdraudējumiem, tie izmanto reputācijas pakalpojumus un tīmekļa lapu satura analīzi. Pārlūkprogrammas Internet Explorer variants ļauj piekļūt Norton Password Manager glabātavas informācijai pārlūkprogrammas lietotāja saskarnē. Tas nodrošina arī meklēšanas lodziņu, lai veiktu meklēšanu Norton Safe Search tīmekļa vietnē. Pārlūkprogrammas Google Chrome variants nodrošina meklēšanas lodziņu, lai veiktu meklēšanu Norton Safe Search tīmekļa vietnē.	1. Ierīces un programmatūras dati, tostarp: tīmekļa pārlūkprogrammas nosaukums, versija un vēlamā valoda; operētājsistēma, versija vai platforma; lietotāja ierīces IP adrese 2. Produkta lietojuma dati, tostarp: tīmekļa vietņu pārlūkošanas aktivitāte; ierobežota tīmekļa vietņu pārlūkošanas vēsture; tīmeklī meklētie vārdi; noklusējuma ievades dažādos meklēšanas lodziņos, kurus pārvalda Norton produkti; meklētājprogrammas rezultāti 3. Sīkfaili, pikseļu tagi, skripti vai līdzīgas tehnoloģijas, kuras datorā vai ierīcē ievieto Norton Safe Search tīmekļa vietne un Norton Home Page tīmekļa vietne	1. Ierīces un programmatūras datus Symantec apstrādā šādiem mērķiem: • pakalpojumu snieguma iespējošanai un optimizēšanai; • licences pārvaldīšanai; • izpratnei par produkta lietošanu un preferencēm, lai personalizētu un uzlabotu lietotāju pieredzi; • vadītu lietotāju programmatūras instalēšanas procesa laikā; • Produktu un Pakalpojumu uzlabojumu sniegšanai, lai labāk aizsargātu lietotāju, lietotāja tīklu, ierīci, datus un identitāti; • klienta apmierinātības uzlabošanai par sniegtajiem pakalpojumiem, izmantojot īpašos un trešo personu zvanu centrus. 2. Produktu lietojuma datus apstrādā Symantec un šie dati tiek apstrādāti Symantec vārdā šādiem mērķiem: • informēt lietotājus par vietnes drošību; • bloķēt pārlūkošanu nedrošās vietnēs; • pakalpojuma lietojuma analizēšanai. 3. Sīkfaili un līdzīgi indeksētāji tiek apstrādāti tālāk norādīto līdzekļu lietošanas preferenču un vēstures nolūkos. Papildinformāciju par sīkfailiem, lūdzu, skatiet iepriekšējā sadaļā ar nosaukumu “Izsekošanas tehnoloģijas, sīkfaili un norādījums par neizsekošanu”, dokumentā Symantec — Norton globālais paziņojums par konfidencialitāti. Turklāt Symantec izmantos apkopotus, neidentificējamus, anonimizētus vai citādi neidentificētus datus, kas iegūti no ievāktiem datiem, piemēram, statistikas: • vispārēju kiberdrošības pētījumu veikšanai; • ļaunprogrammatūras un kiberdraudu atklāšanas uzlabošanai, piemēram, izmantojot failu paraugu analīzi; • ziņojumu par drošības un identitātes zādzības riskiem/tendencēm izsekošanai un publicēšanai; • produktu izvietošanas statistiskās analīzes veikšanai, tostarp tendenču un salīdzinājumu analīzei mūsu apvienotajā lietotāju bāzē; un • produkta veiktspējas uzraudzībai un uzlabošanai attiecībā uz pieejamību un reakcijas laiku.

Norton Password Manager (agrāk Norton Identity Safe)

Produkta/Pakalpojuma apraksts	Datu pieejamība un apkopošana	Datu apstrāde
Produktam Norton Password Manager ir divi varianti — a) produkta Norton Security komponents; un b) pārlūkprogrammas paplašinājums visām populārākajām pārlūkprogrammām, izņemot Internet Explorer. Visi varianti ir paroļu pārvaldnieks, kas pārvalda lietotājvārdus, paroles un citu tiešsaistes darbību veikšanai noderīgu informāciju.	1. Abonenta informācija un ierīces un programmatūras dati, tostarp: tīmekļa pārlūkprogrammas nosaukums, versija un vēlamā valoda; operētājsistēma, versija vai platforma; lietotāja ierīces IP adrese; *citi lietotāja izpausti Personas dati, kuri tostarp var būt lietotājvārdi, paroles, tīmekļa vietņu adreses, fiziskās adreses, maksājumu kontu numuri, informācija par termiņa beigām un brīvas formas teksts 2. Pakalpojuma lietojuma dati, tostarp: tīmekļa vietņu pārlūkošanas aktivitāte; tīmeklī meklētie vārdi; noklusējuma ievades dažādos meklēšanas lodziņos, kurus pārvalda Norton produkti; meklētājprogrammas rezultāti	1. Ierīces un programmatūras datus Symantec apstrādā šādiem mērķiem: • pakalpojumu snieguma iespējošanai un optimizēšanai; • licences pārvaldīšanai; • izpratnei par produkta lietošanu un preferencēm, lai personalizētu un uzlabotu lietotāju pieredzi. • vadītu lietotāju programmatūras instalēšanas procesa laikā; • Produktu un Pakalpojumu uzlabojumu sniegšanai, lai labāk aizsargātu lietotāju, lietotāja tīklu, ierīci, datus un identitāti; • klienta apmierinātības uzlabošanai par sniegtajiem pakalpojumiem, izmantojot īpašos un trešo personu zvanu centrus. 2. Produktu lietojuma datus apstrādā Symantec un šie dati tiek apstrādāti Symantec vārdā šādiem mērķiem: • informēt lietotājus par vietnes drošību; • bloķēt pārlūkošanu nedrošās vietnēs; • pakalpojuma lietojuma analizēšanai. Kritisko kļūdu statistiskās analīzes un pārvaldības nolūkos ar Google Analytics mērījumu protokolu tiek apstrādātas anonimizētas IP adreses un informācija par produktu lietojumu. Noklikšķiniet šeit, lai iegūtu informāciju par Google Analytics datu aizsardzību. Turklāt Symantec izmantos apkopotus, neidentificējamus, anonimizētus vai citādi neidentificētus datus, kas iegūti no ievāktiem datiem, piemēram, statistikas: • vispārēju kiberdrošības pētījumu veikšanai; • ļaunprogrammatūras un kiberdraudu atklāšanas uzlabošanai, piemēram, izmantojot failu paraugu analīzi; • ziņojumu par drošības un identitātes zādzības riskiem/tendencēm izsekošanai un publicēšanai; • produktu izvietošanas statistiskās analīzes veikšanai, tostarp tendenču un salīdzinājumu analīzei mūsu apvienotajā lietotāju bāzē; un • produkta veiktspējas uzraudzībai un uzlabošanai attiecībā uz pieejamību un reakcijas laiku.

Norton Family Premier

Produkta/Pakalpojuma apraksts	Datu pieejamība un apkopošana	Datu apstrāde
Norton Family Premier palīdz aizsargāt aizsargātos lietotājus un viņu ierīces, kuras abonents izvēlas aizsargāt, izmantojot vecāku kontroles. Vecāku kontroles tiek piemērotas ar abonenta norādītiem un ar abonenta pārvaldītiem aizsardzības iestatījumiem un līdzekļiem. Papildinformāciju par Norton Family Premier, lūdzu, skatiet tālāk sadaļā ar nosaukumu "Norton Family Premier papildinformācija"	*1. Abonenta informācija, piemēram: administratora kontaktinformācija, tostarp, bet ne tikai, abonenta vārds, e-pasta adrese un parole, lai aizsargātu abonenta kontu; Personas dati, kurus abonents sniedz Pakalpojuma konfigurēšanas laikā vai jebkurā citā nākamajā pakalpojuma izsaukumā. 2. Ierīces un programmatūras dati, tostarp: Norton Family klienta programmatūras instalācijas statuss abonenta vai aizsargātā lietotāja ierīcē; programmatūras konfigurācija, informācija par produktu un instalācijas statuss; licences statuss, informācija par licences tiesībām, licences ID numurs un licences lietojums; ierīces nosaukums, tips, operētājsistēmas versija, valoda, atrašanās vieta (globālā pozicionēšanas sistēma, GPS), pārlūkprogrammas tips un versija; ierīces aparatūra, programmatūra un programmu klāsts; programmu un datubāzu piekļuves konfigurācijas, politikas prasības un politikas atbilstības statuss, kā arī programmu izņēmumu un darbplūsmas kļūdu žurnāli. *3. Aizsargāta lietotāja informācija, kuru abonents izlemj izpaust uzņēmumam Symantec, tostarp: vārds, dzimums, vecums un dzimšanas gads; avatāra attēli; ar aizsargāto lietotāju saistītā oficiālās personas identifikācijas numura (piemēram, ja pieejams: sociālās apdrošināšanas numura, valsts identifikācijas numura) pēdējie seši cipari, e-pasta adrese, mobilā tālruņa numurs, skolas nosaukums vai jebkāda cita informācija, kuru abonents vēlētos aizsargāt; informācija par pieteikšanos iekārtas kontā, valsts un laika josla. 4. Informācija par aizsargātā lietotāja aktivitāti tīklā, kuru abonents liek uzraudzīt uzņēmumam Symantec, tostarp, pēc abonenta paša izvēles: tiešsaistes un mobilās ierīces darbības un atrašanās vietas; tīmekļa vietnes, kuras aizsargātais lietotājs mēģina apmeklēt, kā arī vietnes, kuras aizsargātais lietotājs nevar apmeklēt, jo Produkts tās bloķē; tiešsaistē meklētie vārdi, kurus aizsargātais lietotājs izmanto; programmas, kuras aizsargātais lietotājs savā ierīcē instalē vai atinstalē, ja abonents ir aktivizējis programmu uzraudzību; aizsargātā lietotāja ierīces lietošanas laiks; *aizsargātā lietotāja profila nosaukums, profila vietrādis URL, vecums, Facebook profila ID un apmeklētie videoklipi; videoklipi, kurus aizsargātais lietotājs skatās vietnē YouTube.com un/vai pakalpojumā Hulu, ja abonents ir aktivizējis video novērošanu.	1. Abonenta informāciju Symantec apstrādā tālāk uzskaitītajiem nolūkiem. • Pakalpojuma Norton Family veiktspējas iespējošana un optimizēšana. • Atbalsta vai atkļūdošanas palīdzības nodrošināšana. • Reklāmas informācijas sūtīšana abonentam saskaņā ar abonenta sniegto atļauju vai ar piemērojamajiem tiesību aktiem citādi sniegto atļauju. • Abonementa Norton konta iestatīšana. 2. Ierīces un programmatūras datus Symantec apstrādā šādiem mērķiem: • Pareiza Produkta darbības nodrošināšana un abonenta pieprasīto Pakalpojumu sniegšana. • Licences pārvaldīšanai. • Sekmīgas Produkta instalēšanas koeficienta novērtēšana un uzlabošana. • Pētniecība un izstrāde, lai uzlabotu Symantec produktus un pakalpojumus, un lai labāk aizsargātu abonentu un aizsargātā lietotāja tīklu, ierīces, datus un identitāti. 3. Aizsargātā lietotāja informācija tiek apstrādāta tālāk uzskaitītajiem nolūkiem. • Abonenta un aizsargātā lietotāja identificēšana un autentificēšana uzņēmumā Symantec. • Palīdzēšana abonentam konstatēt jebkādu aizsargātā lietotāja Personas datu ļaunprātīgu izmantošanu. • Sazināšanās ar abonentu un — ar abonenta atļauju — ar aizsargāto lietotāju, lai nodrošinātu Pakalpojumu. 4. Informācija par aizsargātā lietotāja aktivitātēm tiek apstrādāta tālāk uzskaitītajiem nolūkiem. • Palīdzēšana abonentam uzraudzīt aizsargātā lietotāja ierīces aktivitātes tiešsaistē. • Instalētās ļaunprogrammatūras izdarītā kaitējuma ierobežošana. • Palīdzēšana ievērot abonenta noteiktās kārtulas attiecībā uz aizsargātā lietotāja ierīces aktivitātēm tiešsaistē. • Ļaušana abonentam konstatēt, vai aizsargātais lietotājs ir pakļauts draudiem, izmantojot saziņu tiešsaistē vai ar SMS/MMS. • Palīdzēšana abonentam pasargāt aizsargāto lietotāju no šādiem draudiem. Turklāt Symantec izmantos apkopotus, neidentificējamus, anonimizētus vai citādi neidentificētus datus, kas iegūti no ievāktiem datiem, piemēram, statistikas: • vispārēju kiberdrošības pētījumu veikšanai; • ļaunprogrammatūras un kiberdraudu atklāšanas uzlabošanai, piemēram, izmantojot failu paraugu analīzi; • ziņojumu par drošības un identitātes zādzības riskiem/tendencēm izsekošanai un publicēšanai; • produktu izvietošanas statistiskās analīzes veikšanai, tostarp tendenču un salīdzinājumu analīzei mūsu apvienotajā lietotāju bāzē;

Norton Family Premier papildinformācija

Ja abonents izvēlas aktivizēt šo pakalpojumu, Norton Family neļauj aizsargātajam lietotājam savus Personas datus padarīt publiski pieejamus.

Ja un ciktāl to atļauj piemērojamie tiesību akti tajā valstī vai reģionā, kur atrodas abonents, Symantec var nodrošināt **Īsziņu pārraudzības** pakalpojumu, kas abonentam ļauj bloķēt vai pārraudzīt īsziņas ("SMS") un multiziņas ("MMS"), kuras tiek sūtītas uz aizsargātā lietotāja mobilo tālruni vai no tā, kā arī **Atrašanās vietas uzraudzības pakalpojumu**. SMS un MMS apmaiņas un/vai atrašanās vietas uzraudzīšana, kā arī jebkādas šādas uzraudzības ieraksta izmantošana var tikt ierobežota vai aizliegta ar abonentam piemērojamajiem vietējiem tiesību aktiem. Pirms šī līdzekļa aktivizēšanas abonentam tas ir noteikti jānoskaidro no vietējām iestādēm.

Kad abonents ir iespējojis Atrašanās vietas uzraudzības pakalpojumu, pakalpojums Norton Family izpilda abonenta norādījumus, lai izmantotu GPS, izsekojot abonenta norādīto mobilo ierīci un vācot tās ģeogrāfiskās atrašanās vietas datus. Lai izsekotu, vāktu, lietotu vai izpaustu norādītās ierīces ģeogrāfisko atrašanās vietu, pakalpojumam Norton Family ir nepieciešama abonenta piekrišana, kā arī, iespējams, piekrišana no mobilās ierīces lietotāja, vai piekrišana no personas, kuras aizgādniecībā atrodas šis lietotājs. Attiecīgā piekrišana vai piekrišanas tiek vāktas, izmantojot Norton tiešsaistes portālu, kā arī, iespējams, pašā produktā, un šī piekrišana tiek apstiprināta, kad abonents ievada informāciju par savu maksājumu karti, lai no Symantec tiešsaistē iegādātos Pakalpojumu. Savu piekrišanu varat atsaukt jebkurā laikā. Papildinformāciju par to, kā to izdarīt, lūdzu, skatiet sadaļā "Jūsu konfidencialitātes tiesības", dokumentā Symantec — Norton globālais paziņojums par konfidencialitāti. Pēc Pakalpojuma izbeigšanas abonenta konta informācija saistībā ar šo Pakalpojumu tiek dzēsta.

Kad abonents ir lejupielādējis programmu norādītajā mobilajā ierīcē, Symantec var vākt informāciju par šīs ierīces ģeogrāfisko atrašanās vietu pat tad, ja programma netiek lietota. Šo informāciju par ģeogrāfisko atrašanās vietu mēs izpaužam tikai abonentam, lai abonents varētu atrast ierīci, un šo informāciju mēs apstrādājam tikai ar nolūku sniegt abonenta pieprasītos pakalpojumus un funkcionalitāti. Abonentam nav tiesību izmantot Produkta atrašanās vietas uzraudzības pakalpojumu, lai uzraudzītu datus, atrašanās vietu, aktivitātes un jebkādus citus datus saistībā ar personām, kuras neatrodas abonenta aizgādniecībā. Eiropas Ekonomikas zonā esošajiem abonentiem ir jārunā ar aizsargātajiem lietotājiem, kas atrodas abonentu aizgādniecībā, it īpaši, ja aizsargātajiem lietotājiem ir vairāk nekā 13 gadu, un abonentiem ir jāveic visi nepieciešamie pasākumi, lai nodrošinātu, ka attiecīgais aizsargātais lietotājs saprot, ko nozīmē abonenta veiktā Produkta un saistīto Pakalpojumu lietošana. Izvēloties izmantot Produktu un saistītos Pakalpojumus, tikai abonents ir atbildīgs par visu tiesību aktu un noteikumu ievērošanu, kas ir piemērojami abonenta attiecībām ar aizsargāto lietotāju un aizsargātā lietotāja aizgādniecību.

Īsziņu pārraudzība

Pēc noklusējuma Īsziņu pārraudzība ir izslēgta. Abonentam ir nepieciešams atsevišķi ieslēgt līdzekli "Īsziņu pārraudzība" un instalēt lietotni "Norton Family" mobilajā ierīcē, kur ir paredzēts veikt šo pārraudzīšanu. Kad Īsziņu pārraudzības pakalpojums ir aktivizēts, pakalpojums no norādītās ierīces vāc tālāk uzskaitīto informāciju.

- Pārraugāmās ierīces mobilā tālruņa numurs un mobilā tālruņa numuri citām ierīcēm, ar kurām ierīce sazinās, izmantojot SMS un MMS.
- Norādītajā ierīcē saņemto vai no šīs ierīces sūtīto SMS saturs (attiecībā uz saziņu, izmantojot MMS, Symantec neieraksta un netver nekādu saziņas multivides saturu, bet tikai faktu, ka ir notikusi saziņa, izmantojot MMS).
- Ja pieejams — nosaukums no adrešu grāmatas norādītajā ierīcē, kas ir saistīts ar SMS vai MMS saziņu sūtījušā vai saņēmušā mobilā tālruņa numuru.
- Sarunas datuma/laika laikspiedols.
- Norādītās ierīces atrašanās vieta.
- Bloķēto SMS/MMS ziņojumu notikumu žurnāls, tostarp iesaistīto pušu tālruņa numuri, un saistītie vārdi, ja tādi ir pieejami norādītās ierīces adrešu grāmatā.

Pirms tiek sākta abonenta norādītās mobilās ierīces sūtīto un/vai saņemto SMS vai MMS ziņojumu uzraudzīšana, Symantec uz norādīto ierīci nosūta SMS brīdinājumu, brīdinot ierīces lietotāju, ka Produkts gatavojas izpildīt abonenta norādījumus par norādītajā ierīcē veiktās saziņas SMS un MMS ziņojumu satura ierakstīšanu un uzraudzīšanu. Ja pēc šī SMS brīdinājuma saņemšanas norādītajā ierīcē turpinās SMS vai MMS ziņojumu apmaiņa, ziņapmaiņas ierakstīšana un uzraudzība šajā Paziņojumā aprakstītajiem nolūkiem sākas saskaņā ar abonenta norādījumiem. Šo pašu SMS brīdinājumu Symantec uz norādīto ierīci atkārtoti sūta reizi mēnesī vai katru reizi, kad sākas jauna saruna.

Ja abonents izlemj bloķēt visus SMS vai MMS ziņojumus vai ziņojumus ar noteiktu sarunu biedru, mēs brīdinām norādītās ierīces lietotāju un nosūtam īsziņu sarunu biedram, norādot, ka ziņapmaiņa ir bloķēta un ka ziņu nevar piegādāt.