

Nortons personvernmerknad for produkter og tjenester – *Sist oppdatert 29. april 2019*

Denne merknaden skal leses og gjelder i forbindelse med, og i tillegg til Symantec – Global personvernerklæring fra Norton. Den beskriver de kategorier av data som samles inn av Nortons produkter og tjenester, og for hvilke formål disse datakategoriene blir behandlet. Den er utformet for å gi obligatorisk åpen informasjon både til individuelle Norton-brukere som registrerte og til små og mellomstore bedrifter som er Norton-brukere som dataansvarlige. Vennligst merk deg at datakategorier merket med en stjerne (*) er personopplysninger overført til Symantec med henblikk på levering av korresponderende Norton produktfunksjoner og tjenestefunksjonaliteter. Alle andre datakategorier blir samlet inn av Norton-programvare for behandling i en ikke-identifiserbar form.

Alle Nortons produkter og tjenester holdes til de høye standardene som er angitt i [Symantec – Global personvernerklæring fra Norton](#). Videre, for å informere deg om de unike egenskapene til og spesifikke formålene for enkelte Norton-produkter og -tjenester, i tillegg til en beskrivelse av produktet eller tjenesten, beskriver denne merknaden de personlige dataene vi samler inn og formålene de personlige dataene behandles for.

Hvis noen del eller deler av denne erklæringen er uakseptabel for deg, kan du ikke laste ned, installere eller på annen måte bruke de tilsvarende produktene, tjenestene eller funksjonene deres, og/eller vi ber deg umiddelbart avinstallere eller avbryte bruk av produktene, tjenestene eller funksjonene det gjelder. Du blir bedt om å gjennomgå denne merknaden slik at du kan gi informert og spesifikt samtykke når du laster ned, installerer, aktiverer eller bruker produkt- og tjenestefunksjoner som krever at du oppgir ytterligere personlige data til oss, eller som krever at du samtykker i behandling av slike personlige data, for å kunne dra nytte av spesifikke valgfrie funksjoner i et produkt eller en tjeneste.

Innhold

Norton App Lock.....	2
Norton Clean	2
Norton Error Management.....	2
Norton Community Watch	3
Norton Core.....	4
Norton Mobile Security	5
Norton Security Scan	6
Norton Secure Login.....	7
Norton Ultimate brukerstøtte & Norton Computer Tune-Up	8
Norton Secure VPN (tidligere Norton WiFi Privacy)	9
Nortons sikkerhetsprodukter (Security, Internett Security, One, Antivirus & 360)	10
Norton Safe Search, Norton Home Page, Norton Safe Web.....	11
Norton Security Toolbar	12
Norton Password Manager (tidligere Norton Identity Safe).....	13
Norton Family Premier	14

Norton App Lock

Produkt-/tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
Norton App Lock lar brukeren sikre og beskytte mobilapper ved å låse dem med en PIN-kode, et passord eller et mønster. Hvis mobilenheten er tapt eller stjålet, kan App Lock også konfigureres slik at enhetens frontkamera, hvis det er utstyrt, tar bilde ved tre mislykkede forsøk på å låse opp enheten.	<ol style="list-style-type: none"> 1. Brukers e-postadresse 2. Brukerens PIN-koder for oppsett, passord for mobilapper 3. Etter brukerens valg, bilder basert på innstillinger 	<ol style="list-style-type: none"> 1. Brukerens e-postadresse samles inn og overføres til Symantec for å aktivere behandling av passordgjenoppretting og tilbakestilling med Norton App Lock. 2. 3. Alle andre data som produktet samler inn fra brukerinndata, blir lagret på brukerens enhet.

Norton Clean

Produkt-/tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
Norton Clean er et program som maksimerer lagringen ved å gå gjennom mobilenhetens minnebuffer for å slette annonser og uønskede data for å frigjøre ekstra lagringsplass.	Mobilenhetens unike enhetsidentifikator (IMEI)	IMEI-nummeret hentes fra enheten og sendes til Symantec. Ved overføring blir IMEI-nummeret straks delt opp før ytterligere behandling. Det deles opp for å kunne overvåke unik bruk av produktet. Når dataene er delt opp, kan de ikke spores tilbake til den originale enheten, slik at hverken brukeren eller selve enheten kan spores eller overvåkes.

Norton Error Management

Produkt-/tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
Norton Error Management dokumenterer problemer som oppstår i Norton-produktet. I slike tilfeller kan brukeren velge å rapportere feil til Symantec.	<ol style="list-style-type: none"> 1. Informasjon om datamaskinens status (systemspråk, land og operativsystemets versjon) 2. Prosessene som kjører, statusen deres og informasjon om ytelsen 3. Data fra filer og mapper som var åpne da Norton-produktet oppdaget problemet 	<ol style="list-style-type: none"> 1.-2.-3. Systeminformasjon behandles av Symantec for å korrigere problemet og for å forbedre ytelsen til Norton-produktet. <p>Hvis det oppstår feil på grunn av en sikkerhetsrisiko eller sårbarhet, kan Symantec i enkelte tilfeller utlede og dele bestemte data som ikke er brukerspesifikke eller identifiserende, med sikkerhetssamfunnet i sin helhet, for eksempel forskningsorganisasjoner og andre leverandører av sikkerhetsprogrammer. Formålet med slik deling er å fremme bevissthet, gjenkjenning og forebygging av risikoen. Symantec kan også bruke statistikk utledet fra slik informasjon til å spore og publisere rapporter om trender for sikkerhetsrisikoer.</p>

Norton Community Watch

Produkt-/tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
<p>Norton Community Watch tillater Norton brukere av sikkerhetsprodukter å hjelpe til med å forbedre identifikasjonen og redusere tiden det tar å levere beskyttelse mot nye sikkerhetstrusler. Programmet samler inn valgte sikkerhets- og programdata og sender dataene til Symantec for analyse for å identifisere nye trusler og hvor de kommer fra. Dette programmet hjelper til å bygge et bedre, sterkere sikkerhetsprodukt ved å analysere data sendt av brukeren.</p> <p>Når du blir med i Norton Community Watch-programmet:</p> <ol style="list-style-type: none"> Deltar du i å bygge bedre, sterkere kunnskap om og beskyttelse mot nett-trusler gjennom dataene du og andre deltakere sender inn. Teknologien bruker sofistikerte algoritmer til å beregne en vurdering av sikkerhetsomdømmet for alle filer som lastes ned, installeres eller kjøres på maskinen din, uten å gjøre noe bestemt som angår deg eller noen andre personlig. Nortons brukere av sikkerhetsprodukter får fordelene til denne nye innovative teknologien når et Norton-produkt: <ul style="list-style-type: none"> *a. Blokkerer skadelige nedlastninger med Download Insight. Norton forteller deg om nedlastningen din er kjent for å være sikker eller usikker, eller om den har en ukjent sikkerhetsprofil. Dersom nedlastningen ikke er trygg, handler produktet umiddelbart for å beskytte deg; b. Gir bedre oppdagelseshastighet og reduserer antall falske positive; *c. Kjør raskere skanninger ved hjelp av Norton Insight ved å raskt klarere filer som ble sendt inn, analysert og fastslått som kjente gode filer via Norton Community Watch. Ved å oppgi kritiske sikkerhets- og programdata bidrar du til intelligensen som kreves for å identifisere nye trusler og blokkere dem før de når videre. <p>* Norton Insight er bare tilgjengelig på Windows OS.</p>	<ol style="list-style-type: none"> Maskin-ID (data generert av Symantec) Produktserienummer (data tildelt produktet ditt av Symantec) Norton-kontonummer (data tildelt av Symantec) Filbaner Ikke-kjørbare og flyttbare kjørbare filer som er identifisert som skadelig programvare Nettadresser til nettstedet som Norton-produktet anser som potensiell svindel Nettadressen til nettstedet som brukeren sist besøkte før en nedlastet sikkerhetsrisiko ble installert på datamaskinen Informasjon om prosessene og programmene som kjøres på brukerens enhet fra tid til annen, også når det oppstår en potensiell sikkerhetsrisiko Et utvalg av data sendt fra brukerens enhet som svar på en potensiell sikkerhetsrisiko 	<p>Norton Community Watch er en tjeneste som ventes og administreres av Symantec på serverdelen, overføres alle data som samles inn, til Symantec på følgende måte:</p> <ol style="list-style-type: none"> Maskin-ID er nødvendig for å spore antall unike enheter som brukes på hvert abonnement, for å overvåke og håndheve lisensrettighetene og -kravene. Produktserienummer gis til hver bruker og sørger for at hvert produkt er lisensiert for bruk av Symantec. Norton-kontonummer er nødvendig for å spore antall brukere som abonnerer på spesifikke Norton-produkter. -5. Filbaner og ikke-kjørbare og flyttbare, kjørbare filer blir lagret for å identifisere opprinnelsen og logiske plasseringen av nett-trusler som påvirker eller kommer fra brukerens enhet. -7. Nettadresser brukes til å identifisere nettbaserte kilder til potensielle sikkerhetsrisikoer, og for å forbedre evnen til Symantecs produkter og tjenester til å oppdage skadelige handlinger, skadelige hendelser, falske nettsteder, kriminell programvare og andre former for Internett-sikkerhetstrusler. -9. Enhetsdata brukes til å forbedre Symantecs kunnskap og forståelse av nett-trusler. Enhetsdata behandles også for å gi bedre beskyttelse til brukere av Symantecs produkter og tjenester i fremtiden, og for statistisk analyse av trender innen nettsikkerhet.

Norton Core

Produkt- /tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
<p>Norton Core er en trådløs ruter som gir beskyttelse mot skadelig programvare, virus, hackere og andre nett-trusler for enheter som er koblet til ruterens.</p>	<p>*1. SSID/passord for trådløst nettverk (kryptert)</p> <p>2. Enhetsinformasjon, inkludert alle personlige data som er oppgitt av brukeren ved tildeling av enhetsnavn og, hvis det er oppgitt av brukeren, navnet eller aliaset til personen som enheten er tildelt til, samt brukeragent, data/app-bruker, inkludert enhetstype, produsent og modell, operativsystem og IP-adresse</p> <p>3. Data om enhetsbruk, inkludert data angående tidspunktet for siste bruk av enheten, tiden brukt på Internett for hver tilkoblede enhet og gateway-logger for nettverksforbindelser</p> <p>4. Foreldrekontrollinformasjon og -innstillinger som definert og konfigurert av brukeren, inkludert blokkerte nettsteder, besøkte nettsteder og informasjon om tid og innholdsfilter, samt nettadresser for nettsteder som er bestemt eller anses å være farlige</p> <p>*5. Personlige data som brukeren kan oppgi for å opprette en Norton-konto, inkludert et brukernavn og et valgfritt bilde</p> <p>*6. Personlige data gitt av brukeren for kundestøtte og tilkoblingshjelp, for eksempel bruker-ID, navn, rolle, brukerspesifikke retningslinjer og enhetsinformasjon</p> <p>7. Fjernovervåking av nett-trusler inkludert logger for forsøk på å laste ned skadelige kjørbare filer/mobilapper, oversikt over andre risikofylte hendelser eller handlinger, og artefakter, for eksempel feilvareprøver</p> <p>*8. Brukers kontaktinformasjon, uttrykte preferanser</p> <p>*9. Leveringsadresse og relatert informasjon</p> <p>10. Norton Core muliggjør deltakelse i Norton Community Watch</p>	<p>1. Trådløs nettverksinformasjon behandles for den brukerdefinerte konfigurasjonen av Wi-Fi-nettverket.</p> <p>2. Informasjon om enheten behandles for lisensadministrasjon, for å analysere enheten og enhetens trafikk for å overvåke ruterens tilstand og tilkobling og for å hjelpe deg med å feilsøke den, for å forstå produktbruken og svare på varsler.</p> <p>3. Brukerdata fra enheten blir behandlet med det formål å:</p> <ul style="list-style-type: none"> • Optimalisere av ytelsen til Norton Core; • Informere brukere om sikkerheten til nettstedet; og • Blokkere nettleasing på usikre nettsteder. <p>4. Foreldrekontrollinformasjon og -innstillinger brukes til å håndheve reglene og retningslinjene definert av brukeren for profilene som kontrolleres av brukeren, hjelpe brukeren med å oppdage misbruk av personlige data knyttet til slike profiler og for å kommunisere med brukeren og kontrollerte profiler.</p> <p>5.-6. Brukerkontoinformasjon er samlet inn av Symantec for å oppfylle tjenester som er beskrevet i kunde kontrakten, og gi teknisk støtte og assistanse.</p> <p>7. Fjernovervåking av nett-trusler overføres til Symantec for forskning og utvikling for å forbedre Symantecs produkter og tjenester og gi brukeren bedre beskyttelse av nettverk, enheter, data og identitet.</p> <p>8. Brukers kontaktinformasjon og preferanser blir overført til Symantec for å:</p> <ul style="list-style-type: none"> • Veilede brukeren under programvareinstallasjonen for Norton Core; • Informere brukeren om metoder for å forbedre brukeropplevelsen; • Tilpasse informasjon som vises til brukeren, basert på brukerens preferanser (for eksempel språk og geografisk område); og • Forbedre kundetilfredsheten fra tjenester levert via egne og tredjeparters telefonsentre. <p>9. Leveringsadresse og tilhørende informasjon behandles for å levere Norton Core-maskinvaren til brukeren.</p> <p>10. Når det gjelder informasjon knyttet til Norton Community Watch kan du lese Norton Community Watch-delen i denne merknaden for å få ytterligere detaljer.</p> <p>I tillegg kommer Symantec til å bruke aggregerte, avidentifiserte, anonymiserte eller ellers ikke-identifiserende data hentet fra innsamlede statistiske data, for å:</p> <ul style="list-style-type: none"> • Følge opp generelle undersøkelser av nettsikkerheten; • Forbedre påvisning av skadelig programvare og nett-trusler, f.eks. gjennom analyse av filprøver; • Spore og publisere rapporter om sikkerhet og risikoer/trender innen identitetstyveri; • Gjennomføre statistisk analyse av produktutplassering, inkludert analyse av trender og sammenligninger i vår aggregerte brukerbase; • Overvåke og forbedre ytelsen til produktet når det gjelder tilgjengelighet og responstid; • Forstå frekvensen av produktrelatert kommunikasjon for å optimalisere den generelle brukeropplevelsen; og • Oppnå innsikt i andre forretninger og markeder som ikke er knyttet til brukeren, og som er relevante for å forbedre ytelsen til vår virksomhet.

Norton Mobile Security

Produkt-/tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
<p>Med Norton Mobile Security får beskyttede brukere og enheter som abonnenten velger å beskytte, beskyttelse for smarttelefoner og nettbrett mot digitale trusler, gjenoppretting for mistede eller stjålne enheter og gjenoppretting av kontaktinformasjon</p>	<p>1. Beskyttede brukeres data på mobilenheter, inkludert utstyrsidentifikatorer (f.eks. IMEI, Wi-Fi-MAC-adresse, UDID), abonnentinformasjon, mobiltelefonnummer og annen beskyttet brukerkontaktinformasjon, enhetsnavn/-type og produsent, operativsystemtype og -versjon, nettverkstype, opprinnelsesland, brukerstøtterapport-ID, brukerinstallerte sertifikater, nettsteders domenenavn og tilknyttede SSL-sertifikatkjeder fra enheten og IP-adressen</p> <p>2. Bruksdata, for eksempel informasjon om nedlasting og brukshyppighet, loggdata og informasjonskapsler, og nettverkstjenesteinformasjon om hvordan brukeren kobler seg til nettverkstjenestene</p> <p>3. Navnene på filer og apper på brukers enhet hver gang produktet utfører en skanning, inkludert skannede apper som ikke er i Symantecs database over kjente apper, for å beskytte brukeren mot skadelig programvare eller risikofylte funksjoner, samt innhold i kalender og SD-kort, hvis det er tilgjengelig</p> <p>4. Nettadresser til nettslesing, historikk og bokmerker</p> <p>*5. Per brukers valg, kontakter på brukers enhet, inkludert samtale- og SMS-logger</p> <p>6. Innstillinger for telefonsamtaler og enhetslyd</p> <p>*7. Enhetsens posisjonsdata</p>	<p>1. Data fra mobilenheten, abonnentinformasjon og beskyttet brukerkontaktinformasjon behandles for å:</p> <ul style="list-style-type: none"> • Aktivere og optimalisere ytelsen til produktet; • Godkjenne den beskyttede brukers identitet for Symantec; • Veilede brukeren under programvareinstallasjonen; • Kommunisere med den beskyttede brukeren for å yte tjenesten; • Utføre lisensadministrasjon; og • Forbedre kundetilfredsheten fra tjenester levert via egne og tredjeparters telefonsentre. <p>2. Brukerdata blir behandlet for å: Forstå produktbruk og preferanser for å tilpasse og forbedre brukeropplevelsen.</p> <p>3. Fil, programnavn, kalender (for eksempel nettadresser i invitasjoner) og SD-kortinnhold behandles for å:</p> <ul style="list-style-type: none"> • Varsle brukeren om potensielt skadelige apper; • Skanne enheten for skadelig programvare; og • Slette personlig innhold fra enheten hvis brukeren velger å aktivere og kjøre kommandoen for produktets utvisningskommando. <p>4. Nettslesingsdata behandles for å:</p> <ul style="list-style-type: none"> • Informere brukere om sikkerheten på nettsteder; • Blokkere nettslesing på usikre nettsteder; og • Slette nettslesingslogg og bokmerker hvis brukeren velger å bruke produktets nettbeskyttelsesfunksjon eller utvisningskommando. <p>5. Kontakter, inkludert samtale- og SMS-logger på brukers enhet, behandles for å levere funksjonene for blokkering av anrop/tekstmeldinger, hvis brukeren velger å bruke dem.</p> <p>6. Telefoninnstillinger brukes til å blokkere innkommende anrop fra kontakter eller for å endre enhets lydinnstillinger hvis brukeren velger å aktivere og bruke produktets blokkeringsfunksjon og/eller ropekommando.</p> <p>7. 8. Enhetsposisjon og bildedata kan hentes på den beskyttede brukers forespørsel for å finne brukers enhet når enheten mistes eller blir stjålet. Produktet gir også abonnenten fjernkommandoer for å finne den beskyttede brukers enhet hvis den mistes eller blir stjålet. I visse tilfeller når enheten blir rapportert som mistet eller stjålet, låses enheten eksternt. Eventuelt kan produktet lukkes når som helst når enheten er rapportert som mistet eller stjålet. Med tillatelsen fra den beskyttede brukeren kan en logg av opptil de siste ti kjente posisjonene til enheten lagres for å la den beskyttede brukeren spore de siste bevegelsene til enheten, selv om produktet ikke er i bruk.</p> <p>9. Sikkerhetskopidata behandles for å levere produktets funksjoner for sikkerhetskopiering og gjenoppretting, hvis brukeren velger å bruke dem.</p> <p>I tillegg kommer Symantec til å bruke aggregerte, avidentifiserte, anonymiserte eller ellers ikke-identifiserende data hentet fra innsamlede statistiske data, for å:</p> <ul style="list-style-type: none"> • Følge opp generelle undersøkelser av nettsikkerheten; • Forbedre påvisning av skadelig programvare og nett-trusler, f.eks. gjennom analyse av filprøver; • Spore og publisere rapporter om sikkerhet og risikoer/trender innen identitetstyveri;

	<p>*8. Produktet kan også konfigureres slik at når enheten blir rapportert som mistet eller stjålet, kan enhetens frontkamera (hvis det er utstyrt) ta et bilde hvis enheten fortsatt blir brukt, hvis feil passord skrives inn etter ett mislykket forsøk på å låse opp enheten, eller hvis enheten slås på etter at den er slått av</p> <p>9. Sikkerhets kopi av dataene på mobilenheten, inkludert kontakter, anropslogg, telefoner og tekstmeldinger</p>	<ul style="list-style-type: none"> • Gjennomføre statistisk analyse av produktutplassering, inkludert analyse av trender og sammenligninger i vår aggregerte brukerbase; • Overvåke og forbedre ytelsen til produktet når det gjelder tilgjengelighet og responstid; • Forstå frekvensen av produktrelatert kommunikasjon for å optimalisere den generelle brukeropplevelsen; og • Oppnå innsikt i andre forretninger og markeder som ikke er knyttet til brukeren, og som er relevante for å forbedre ytelsen til vår virksomhet.
--	--	--

Norton Security Scan

Produkt-/tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
<p>Norton Secure Scan skanner endepunktsenheter eller enheter valgt av brukeren, identifiserer potensielle utfordringer eller risikoer, og anbefaler produkter og løsninger til brukeren.</p>	<p>1. Maskin-ID (data generert internt av Symantec); Installerer/avinstallerer funksjonen til enheten; enhetsinformasjon og data for brukerdata for brukerdata/appbrukere, inkludert produkttype, versjon av operativsystem, språk i operativsystemet, produsent og modell; operativsystem; og tilhørende geografisk informasjon</p> <p>2. Overvåkingsinformasjon om filer som er skannet, brukeropplevelse og trusler som er funnet, fikset og gjenværende; dato og klokkeslett for skanning etter innsending; statusinformasjon om installasjon og drift, som kan inkludere personlige data som tilfeldigvis befinner seg i en filbane eller et mappenavn</p>	<p>1. Maskin-ID og tilhørende informasjon brukes av Symantec for å:</p> <ul style="list-style-type: none"> • Veilede brukeren under programvareinstallasjonen; • Kommunisere med brukeren for å yte tjenesten; • Forstå tjenestebruk og preferanser for å tilpasse og forbedre brukeropplevelsen. <p>2. Informasjon fra fjernovervåking blir brukt av Symantec for å:</p> <ul style="list-style-type: none"> • Aktiverer og optimaliserer ytelsen til tjenesten; og • Undersøke og utvikle for å forbedre Symantecs produkter og tjenester og bedre å beskytte brukerens nettverk, enheter, data og identitet. <p>I tillegg kommer Symantec til å bruke aggregerte, aidentifiserte, anonymiserte eller ellers ikke-identifiserende data hentet fra innsamlede statistiske data, for å:</p> <ul style="list-style-type: none"> • Følge opp generelle undersøkelser av nettsikkerheten; • Forbedre påvisning av skadelig programvare og nett-trusler, f.eks. gjennom analyse av filprøver; • Spore og publisere rapporter om sikkerhet og risikoer/trender innen identitetstyveri; • Gjennomføre statistisk analyse av produktutplassering, inkludert analyse av trender og sammenligninger i vår aggregerte brukerbase; • Overvåke og forbedre ytelsen til produktet når det gjelder tilgjengelighet og responstid; • Forstå frekvensen av produktrelatert kommunikasjon for å optimalisere den generelle brukeropplevelsen; og • Oppnå innsikt i andre forretninger og markeder som ikke er knyttet til brukeren, og som er relevante for å forbedre ytelsen til vår virksomhet.

Norton Secure Login

Produkt-/tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
<p>Norton Secure Login (NSL) er en identitetsleverandør som leverer en enkel, sikker og sentralisert måte å godkjenne brukere på. Symantec gir en infrastruktur for identitetsbehandling for millioner av brukere på ulike Norton-produkter.</p>	<p>*1. Personlige data for å verifisere brukerens identitet, som postadresse, telefonnummer, fødselsdato og/eller kredittkortnummer; brukerkontaktinformasjon; eventuelle personopplysninger i tillegg som brukeren kan legge inn på brukerens Norton-konto, eller som brukeren kan gi for kundestøtte og tilkoblingshjelp, for eksempel navn og enhetsinformasjon</p> <p>2. Enhets-, produkt- og tjenestedatainformasjon og data for brukerens agentdata/app-brukeragent, inkludert produkttype; produsent; modell; operativsystem og -versjon; informasjon om enheten og data for brukerdata for brukerdata/app-brukeragenter, inkludert produkttype; produsent; modell; operativsystem og versjon; data om ytelse ved kjøring; installerte apper; tilhørende geografisk informasjon, MAC-adresse og IP-adresse</p> <p>3. Bruksdata angående bruk av Internett, for eksempel nettadresser og IP-adresser til besøkte nettsteder, søkeord og -resultater, og informasjon om potensielle sikkerhetsrisikoer (inkludert nettadresser og IP-adresser på nettsteder som anses potensiell svindel, som kan inneholde personlige data nettsiden forsøker å oppnå uten brukerens tillatelse)</p>	<p>1. Personlige data behandles av Symantec for å:</p> <ul style="list-style-type: none"> • Godkjenne brukerens identitet for Symantec eller for å stole på tredjeparter som bruker Norton Security Login; • Utstede legitimasjon og/eller unngått svindeltransaksjoner i brukerens navn; • Veilede brukeren under programvareinstallasjonen; • Kommunisere med brukeren for å yte tjenesten, inkludert kundestøtte og assistanse; og • Forbedre kundetilfredsheten fra tjenester levert via egne og tredjeparters telefonsentre. <p>2. Enhets-, produkt- og tjenesteinformasjon behandles av Symantec for å:</p> <ul style="list-style-type: none"> • Aktivere og optimalisere ytelsen til produkter og tjenester; • Utføre lisensadministrasjon; og • Forstå produktbruk og preferanser for å tilpasse og forbedre brukeropplevelsen. <p>3. Brukerdata behandles av Symantec for å:</p> <ul style="list-style-type: none"> • Informere brukere om sikkerheten på nettsteder; • Blokkere nettlæsning på usikre nettsteder; og • Undersøke og utvikle for å forbedre Symantecs produkter og tjenester og bedre å beskytte brukerens nettverk, enheter, data og identitet. <p>I tillegg kommer Symantec til å bruke aggregerte, aidentifiserte, anonymiserte eller ellers ikke-identifiserende data hentet fra innsamlede statistiske data, for å:</p> <ul style="list-style-type: none"> • Følge opp generelle undersøkelser av nettsikkerheten; • Forbedre påvisning av skadelig programvare og nett-trusler, f.eks. gjennom analyse av filprøver; • Spore og publisere rapporter om sikkerhet og risikoer/trender innen identitetstyveri; • Gjennomføre statistisk analyse av produktutplassering, inkludert analyse av trender og sammenligninger i vår aggregerte brukerbase; • Overvåke og forbedre ytelsen til produktet når det gjelder tilgjengelighet og responstid; • Forstå frekvensen av produktrelatert kommunikasjon for å optimalisere den generelle brukeropplevelsen; og • Oppnå innsikt i andre forretninger og markeder som ikke er knyttet til brukeren, og som er relevante for å forbedre ytelsen til vår virksomhet.

Norton Ultimate brukerstøtte & Norton Computer Tune-Up

Produkt-/tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
<p>Norton Ultimate brukerstøtte lar brukeren kontakte en ekspert for å få hjelp med tekniske problemer som spenner fra nettverksoppsett til enhetsdiagnostikk og feilsøking.</p> <p>Norton Computer Tune-Up er en funksjon i Norton Ultimate brukerstøtte som bidrar til å holde brukerens enhet som ny, ved hjelp av diagnostikk.</p>	<p>*1. Forespørselsinformasjonen du oppgir til Symantec-servicerepresentanter over telefonen eller som du skriver inn i Symantecs nettgrensesnitt når du ber om Norton Services</p> <p>2. Systeminformasjon inkluderer: Typen og versjonen av operativsystemet og nettleseren som brukes på enheten din; hvorvidt en brannmur er aktiv; hvorvidt antivirusprogramvare er installert, kjører og er oppdatert; minne- og diskplass, konfigurasjon av proxy-server og katalogoppføringer for Support Software-verktøyet; nettleserinformasjon, inkludert innstillinger for sikkerhet og midlertidige filer; aktive porter, vertsfil og innstillinger for nettverksgrensesnitt på enheten; informasjon om installerte programmer og aktive prosesser; loggfilinformasjon for program og operativsystem, og registerdata</p> <p>3. Diagnostikkinformasjon inkluderer: Antallet filer skannet, trusler funnet og trusler fikset av Support Software-verktøyet; trusseltyper som er funnet; sikkerhetsstatusen (god/rimelig/dårlig) til enheten, som fastslått av Support Software-verktøyet; antallet og typen trusler som gjenstår, som ikke er fikset av Support Software-verktøyet</p>	<p>1. Etterspurt informasjon behandles av Symantec for å:</p> <ul style="list-style-type: none"> • Kommunisere med brukeren for å yte tjenesten; • Forstå produktbruk og preferanser for å tilpasse og forbedre brukeropplevelsen; og • Forbedre kundetilfredsheten fra tjenester levert via egne og tredjeparters telefonsentre. <p>2. Systeminformasjon behandles av Symantec for å:</p> <ul style="list-style-type: none"> • Leverer tjenester etterspurt av brukeren; • Aktivere og optimalisere ytelsen til tjenesten; og • Veilede brukeren under bruken av tjenestene; <p>3. Diagnostikkinformasjon behandles av Symantec for å:</p> <ul style="list-style-type: none"> • Informere brukeren om resultatet av de utførte tjenestene; og • Undersøke og utvikle for å forbedre Symantecs produkter og tjenester og bedre å beskytte brukerens nettverk, enheter, data og identitet. <p>I tillegg kommer Symantec til å bruke aggregerte, aidentifiserte, anonymiserte eller ellers ikke-identifiserende data hentet fra innsamlede statistiske data, for å:</p> <ul style="list-style-type: none"> • Følge opp generelle undersøkelser av nettsikkerheten; • Forbedre påvisning av skadelig programvare og nett-trusler, f.eks. gjennom analyse av filprøver; • Spore og publisere rapporter om sikkerhet og risikoer/trender innen identitetstyveri; • Gjennomføre statistisk analyse av produktutplassering, inkludert analyse av trender og sammenligninger i vår aggregerte brukerbase; • Overvåke og forbedre ytelsen til produktet når det gjelder tilgjengelighet og responstid; • Forstå frekvensen av produktrelatert kommunikasjon for å optimalisere den generelle brukeropplevelsen; og • Oppnå innsikt i andre forretninger og markeder som ikke er knyttet til brukeren, og som er relevante for å forbedre ytelsen til vår virksomhet.

Norton Secure VPN (tidligere Norton WiFi Privacy)

Produkt-/tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
<p>Norton Secure VPN beskytter brukers enheter og beskytter brukers data ved å kryptere brukers informasjon på en hvilken som helst Internett-tilkobling og bevare brukers personvern.</p>	<p>1. Abonnementinformasjon og data om mobilenhet, inkludert navn, type, versjon av operativsystem og språk;</p> <p>2. Samlet båndbreddebruk;</p> <p>3. Midlertidig bruksdata som hjelper deg med å feilsøke et problem med tjenesten.</p>	<p>1. Abonnementinformasjon og data om mobilenhet behandles av Symantec for å:</p> <ul style="list-style-type: none"> • Aktivere og optimalisere ytelsen til tjenesten; • Forstå produktbruk og preferanser for å tilpasse og forbedre brukeropplevelsen; • Veilede brukeren under installasjon av programvaren og bruk av tjenesten; • Kommunisere med brukeren for å yte tjenesten; • Påminne brukeren om å beskytte informasjonen brukeren overfører; og • Forbedre kundetilfredsheten fra tjenester levert via egne og tredjeparters telefonsentre. <p>2. Data om båndbreddebruk behandles av Symantec i forbindelse med fakturering, nettverksoperasjoner og kundestøtte.</p> <p>3. Midlertidige bruksdata behandles av Symantec for å:</p> <ul style="list-style-type: none"> • Velge den mest hensiktsmessige serveren for å koble til; og • Undersøke og utvikle for å forbedre Symantecs produkter og tjenester og bedre å beskytte brukers nettverk, enheter, data og identitet. <p>Under bruk av Norton Secure VPN, sender vi brukers Internett-trafikk gjennom Symantecs nettverk, som er et «No Log»-nettverk. Dette betyr at Symantec ikke lagrer brukers opprinnelige IP-adresse når Norton Secure VPN er koblet til, og derfor kan ikke Symantec identifisere hver enkelt enhet. Symantecs automatiserte regelbaserte trafikkstyring kan kreve sanntidsanalyse av datatrafikk, inkludert destinasjonsnettsteder eller IP-adresser og opprinnelige IP-adresser, men ingen logg opprettholdes angående denne informasjonen. Symantec lagrer ikke informasjon om programmer, tjenester eller nettsteder som brukeren laster ned, bruker eller besøker. Siden Symantec forvalter et globalt nettverk, kan brukers Internett-trafikk bli dirigert gjennom et eller flere forskjellige land som forklart i Symantec – Global personvernerklæring fra Norton.</p> <p>I tillegg kommer Symantec til å bruke aggregerte, avidentifiserte, anonymiserte eller ellers ikke-identifiserende data hentet fra innsamlede statistiske data, for å:</p> <ul style="list-style-type: none"> • Følge opp generelle undersøkelser av nettsikkerheten; • Forbedre påvisning av skadelig programvare og nett-trusler, f.eks. gjennom analyse av filprøver; • Spore og publisere rapporter om sikkerhet og risikoer/trender innen identitetstyveri; • Gjennomføre statistisk analyse av produktutplassering, inkludert analyse av trender og sammenligninger i vår aggregerte brukerbase; • Overvåke og forbedre ytelsen til produktet når det gjelder tilgjengelighet og responstid; • Forstå frekvensen av produktrelatert kommunikasjon for å optimalisere den generelle brukeropplevelsen; og • Oppnå innsikt i andre forretninger og markeder som ikke er knyttet til brukeren, og som er relevante for å forbedre ytelsen til vår virksomhet.

Nortons sikkerhetsprodukter (Security, Internett Security, One, Antivirus & 360)

Dette avsnittet dekker Norton Security (Standard, Deluxe og Premium), Norton Internett Security, Norton One, Norton Antivirus, Norton Antivirus Basic, Norton 360, Norton 360PE og Norton 360MD.

Produkt-/tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
<p>Nortons sikkerhetsprodukter gir sikkerhet til endepunkt og som beskytter mot skadelig programvare, spionprogramvare, virus og andre trusler på nettet.</p>	<ol style="list-style-type: none"> 1. Abonnementinformasjon og data, inkludert *personopplysninger som brukeren kan legge inn for å opprette en Norton-konto, for eksempel et brukernavn og et valgfritt bilde; eventuelle *personopplysninger som brukeren inkluderer ved tildeling av enhetsnavn og, hvis det er oppgitt, navnet eller aliaset til personen som enheten er tildelt, og data om brukeren agentdata/appbrukeragent, inkludert produkttype, produsent, og modell; operativsystem og versjon; programmer og versjoner; tilhørende geografisk informasjon, MAC-adresse, maskin-ID og IP-adresse; statusinformasjon om installasjon og drift, som kan inneholde personlige data i tilfelle dette tilfeldigvis ligger i et fil- eller mappenavn; eventuelle ytterligere personlige data som brukeren gir til Symantec for kundestøtte og tilkoblingshjelp, for eksempel bruker-ID, navn, rolle, retningslinjer og informasjon om utstyr 2. Data angående bruk av Internett, for eksempel nettadresser og IP-adresser til besøkte nettsteder, søkeord og -resultater, og informasjon om potensielle sikkerhetsrisikoer (inkludert nettadresser og IP-adresser på nettsteder som anses potensiell svindel, som kan inneholde personlige data nettsiden forsøker å oppnå uten brukeren tillatelse) 3. Data om bruk av enheten og diagnostikk, inkludert: Data angående tidspunktet for siste bruk av utstyret, tid brukt på Internett for hver tilkoblede enhet og logger over inngangsporter som angir aktiviteter på nettverksforbindelser; kjørbare filer som er identifisert som potensiell skadelig programvare, som kan inkludere personlige data som er hentet inn av skadelig programvare uten brukeren tillatelse; e-postmeldinger som er rapportert som søppelpost eller feilidentifisert som søppelpost, som er sendt til Symantec med brukeren tillatelse; «krasjdump»-informasjon eller informasjon i en rapport som brukeren kan velge å sende til Symantec når produktene og tjenestene støter på et problem, som kan inkludere systemspråket, landets lokalitet, operativsystem og prosesser/filer som kjører på tidspunktet da feilen oppsto 4. Foreldrekontrollinformasjon og -innstillinger som definert og konfigurert av brukeren, inkludert blokkerte nettsteder, besøkte nettsteder og informasjon om tid og innholdsfilter, samt nettadresser for nettsteder som er bestemt eller anses å være farlige. 	<ol style="list-style-type: none"> 1. Abonnementinformasjon og enhetsdata behandles av Symantec for å: <ul style="list-style-type: none"> • Aktivere og optimalisere ytelsen til produktet og tjenesten; • Godkjenne den beskyttede brukeren identitet for Symantec; • Forstå produktbruk og preferanser for å tilpasse og forbedre brukeropplevelsen; • Veilede brukeren under programvareinstallasjonen; • Kommunisere med brukeren for å yte tjenesten; • Utføre lisensadministrasjon; og • Forbedre kundetilfredsheten fra tjenester levert via egne og tredjeparters telefonsentre. 2. Informasjon om nettbruken blir behandlet for å: <ul style="list-style-type: none"> • Informere brukeren om sikkerheten til nettstedet; og • Blokkere nettlese på usikre nettsteder. 3. Enhetens bruks- og diagnostikkdata behandles av Symantec for å: <ul style="list-style-type: none"> • Forstå produktbruken; • Levere beskyttelsesfunksjonene til produkter og tjenester; og • Undersøke og utvikle for å forbedre Symantecs produkter og tjenester og bedre å beskytte brukeren nettsted, enheter, data og identitet. 4. Foreldrekontrollinformasjon og -innstillinger brukes til å håndheve reglene og retningslinjene definert av brukeren for profilene som kontrolleres av brukeren, hjelpe brukeren med å oppdage misbruk av personlige data knyttet til slike profiler og for å kommunisere med brukeren og kontrollerte profiler. <p>I tillegg kommer Symantec til å bruke aggregerte, aidentifiserte, anonymiserte eller ellers ikke-identifiserende data hentet fra innsamlede statistiske data, for å:</p> <ul style="list-style-type: none"> • Følge opp generelle undersøkelser av nettsikkerheten; • Forbedre påvisning av skadelig programvare og nett-trusler, f.eks. gjennom analyse av filprøver; • Spore og publisere rapporter om sikkerhet og risikoer/trender innen identitetstyveri; • Gjennomføre statistisk analyse av produktutplassering, inkludert analyse av trender og sammenligninger i vår aggregerte brukerbases; • Overvåke og forbedre ytelsen til produktet når det gjelder tilgjengelighet og responstid; • Forstå frekvensen av produktrelatert kommunikasjon for å optimalisere den generelle brukeropplevelsen; og • Oppnå innsikt i andre forretninger og markeder som ikke er knyttet til brukeren, og som er relevante for å forbedre ytelsen til vår virksomhet.

Norton Safe Search, Norton Home Page, Norton Safe Web

Produkt-/tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
<p>Norton Safe Search er en nettside for søkemotorer som bidrar til å beskytte brukeren mot usikre nettsted ved å filtrere søkeresultatene og gi nettstedets sikkerhetsvurderinger til brukeren for å gi en sikrere nettlesingsopplevelse. Det er også en nettleserutvidelse som gir tilgang til Norton Safe Search-nettsiden på ulike måter. Forskjellige versjoner av denne utvidelsen kan, etter brukerens valg, enten:</p> <p>a) overstyre nettleserens standard søkemotor til Norton Safe Search-nettstedet eller;</p> <p>b) overstyre nettleserens standard søkemotorinnstilling til Norton Safe Search-nettsiden OG overstyre nettleserens standard hjemmeside + nye faneinnstillinger til Nortons hjemmeside.</p> <p>Norton Home Page er en nettleserutvidelse og standard hjemmeside som aktiverer Norton Safe Search-nettstedet.</p> <p>Norton Safe Web er en nettleserutvidelse som brukeren velger å bruke for å overvåke surfeaktiviteten og innhold på nettsiden. Den bruker omdømmetjenester og innholdsanalyse for</p>	<p>1. Abonnementinformasjon, enhets- og programvaredata, inkludert: Nettlesernavn, versjon og foretrukket språk; operativsystem, versjon eller plattform; brukerens IP-adresse</p> <p>2. Data over tjenestebruken, inkludert: Lenker i sosiale medier og web e-post; Nettstedets surfeaktivitet; søkeord på nettet; standardinn ganger i forskjellige søkebokser som forvaltes av Norton-produktene; søkemotorresultater</p> <p>3. Informasjonskapsler, pikseletiketter, skript eller lignende teknologier som er plassert på datamaskinen eller enheten av Norton Safe Search-nettsiden og på Nortons hjemmeside</p>	<p>1. Abonnementinformasjon, enhets- og programvaredata behandles av Symantec for å:</p> <ul style="list-style-type: none"> • Aktivere og optimalisere ytelsen til tjenesten; • Utføre lisensadministrasjon; • Forstå produktbruk og preferanser for å tilpasse og forbedre brukeropplevelsen; • Veilede brukeren under programvareinstallasjonen; • Leverer produkt- og serviceforbedringer for å gi brukeren samt brukerens nettverk, enhet, data og identitet bed beskyttelse; og • Forbedre kundetilfredsheten fra tjenester levert via egne og tredjeparters telefonsentre. <p>2. Tjenestebruksdata behandles av Symantec og på vegne av Symantec for å:</p> <ul style="list-style-type: none"> • Informere brukeren om sikkerheten til nettstedet; • Blokkere nettlesing på usikre nettsteder; og • Analysere bruken av tjenesten. <p>Brukerens søk gjennom Norton Safe Search produktet sendes videre til våre tredjeparts søkepartnere Oath/Yahoo! (for USA og Canada) og IACI (utenfor USA/Canada) for at søkehistorikken skal leveres til deg. . Våre tredjepartspartnere kan også samle inn informasjon direkte i henhold til aktiviteten din på Norton Safe Search. Våre tredjeparts partnere samler inn slike data som datakontrollører for å behandle søket ditt. Slik innsamling av data er underlagt personvernreglene, -erklæringen og merknaden fra tredjeparts partnerne.</p> <p>For at Norton Safe Search skal bli levert til deg, blir søket ditt rettet mot vår tredjeparts partner (dvs. ikke et Symantec-selskap), der en slik tredjeparts partner behandler søket ditt. Våre tredjepartspartnere kan også samle inn informasjon direkte fra deg via aktiviteten din på Norton Safe Search («tredjepartsdata»). Tredjeparts partneren er datakontrolløren som behandler søket ditt. Derfor er det vår tredjeparts partner, i stedet for Symantec, som bestemmer hvordan tredjeparts data blir samlet inn, brukt, oppgitt, beholdt eller på annen måte bearbeidet. Tredjepartsdataene dine er underlagt tredjepartners personvernerklæring(er) for behandling av dataene dine for å utføre søket. Se personvernerklæringene fra vår tredjeparts partner.</p> <p>3. Informasjonskapsler og lignende sporinger behandles for å følge innstillinger for funksjonsbruk og historikk. For å få mer informasjon om informasjonskapsler se avsnittet ovenfor med tittelen «Sporingsteknologi, informasjonskapsler og deaktivering av sporing»-delen av Symantec – Global-personvernerklæring for Norton.</p> <p>Anonymiserte IP-adresser og informasjon om produktbruk behandles av Google Analytics' måleprotokoll for statistisk analyse og behandling av kritiske feil. Klikk her for å få informasjon om sikkerhetstiltak for data i Google Analytics.</p> <p>I tillegg kommer Symantec til å bruke aggregerte, avidentifiserte, anonymiserte eller ellers ikke-identifiserende data hentet fra innsamlede statistiske data, for å:</p> <ul style="list-style-type: none"> • Følge opp generelle undersøkelser av nettsikkerheten; • Forbedre påvisning av skadelig programvare og nett-trusler, f.eks. gjennom analyse av filprøver; • Spore og publisere rapporter om sikkerhet og risikoer/trender innen identitetstyveri; • Gjennomføre statistisk analyse av produktplassing, inkludert analyse av trender og sammenligninger i vår aggregerte brukerbase; og

<p>nettsider til å beskytte brukeren mot skadelig nettsideinnhold, nettfisking og andre trusler.</p>		<ul style="list-style-type: none"> • Overvåke og forbedre ytelsen til tjenesten når det gjelder tilgjengelighet og responstid.
--	--	---

Norton Security Toolbar

Produkt-/tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
<p>Norton Security Toolbar har to varianter a) et tillegg til Microsoft Internett Explorer og b) en nettleserutvidelse til Google Chrome. Begge varianter blir brukt av brukeren for å overvåke brukeren surfeaktivitet og nettsideinnhold. De bruker omdømmetjenester og innholdsanalyse for nettsider for å beskytte brukeren mot skadelig nettsideinnhold, nettfiske og andre trusler.</p> <p>Internett Explorer-varianten tillater tilgang og bruk av Norton Password Manager-hvelvinformasjon i nettleserens brukergrensesnitt. Den har også en søkeboks for å søke på Norton Safe Search-nettstedet. Google Chrome-varianten har en søkeboks for å søke på Norton Safe Search-nettstedet.</p>	<ol style="list-style-type: none"> 1. Enhets- og programvaredata, inkludert: Nettleseravn, versjon og foretrukket språk; operativsystem, versjon eller plattform; brukeren IP-adresse 2. Data over produktbruken, inkludert: Nettstedets surfeaktivitet; begrenset nettlesingshistorikk; søkeord på nettet; standardinnganger i forskjellige søkebokser som forvaltes av Norton-produktene; søkemotorresultater 3. Informasjonskapsler, pikseletiketter, skript eller lignende teknologier som er plassert på datamaskinen eller enheten av Norton Safe Search-nettsiden og på Nortons hjemmeside 	<ol style="list-style-type: none"> 1. Enhets- og programvaredata behandles av Symantec for å: <ul style="list-style-type: none"> • Aktivere og optimalisere ytelsen til tjenesten; • Utføre lisensadministrasjon; • Forstå produktbruk og preferanser for å tilpasse og forbedre brukeropplevelsen; • Veilede brukeren under programvareinstallasjonen; • Levere produkt- og serviceforbedringer for å gi brukeren samt brukeren nettværk, enhet, data og identitet bed beskyttelse; og • Forbedre kundetilfredsheten fra tjenester levert via egne og tredjeparters telefonsentre. 2. Produktbruksdata behandles av Symantec og på vegne av Symantec for å: <ul style="list-style-type: none"> • Informere brukeren om sikkerheten til nettstedet; • Blokkere nettlesing på usikre nettsteder; og • Analysere bruken av tjenesten. 3. Informasjonskapsler og lignende sporinger behandles for å følge innstillinger for funksjonsbruk og historikk. For å få mer informasjon om informasjonskapsler se avsnittet ovenfor med tittelen «Sporingsteknologi, informasjonskapsler og deaktivering av sporing»-delen av Symantec – Global-personvernerklæring for Norton. <p>I tillegg kommer Symantec til å bruke aggregerte, aidentifiserte, anonymiserte eller ellers ikke-identifiserende data hentet fra innsamlede statistiske data, for å:</p> <ul style="list-style-type: none"> • Følge opp generelle undersøkelser av nettsikkerheten; • Forbedre påvisning av skadelig programvare og nett-trusler, f.eks. gjennom analyse av filprøver; • Spore og publisere rapporter om sikkerhet og risikoer/trender innen identitetstyveri; • Gjennomføre statistisk analyse av produktplassing, inkludert analyse av trender og sammenligninger i vår aggregerte brukerbase; og • Overvåke og forbedre ytelsen til tjenesten når det gjelder tilgjengelighet og responstid.

Norton Password Manager (tidligere Norton Identity Safe)

Produkt-/tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
<p>Norton Password Manager har to varianter: a) en komponent av Norton Security og b) nettleseutvidelser for alle de store nettleserne bortsett fra Internett Explorer. Alle varianter er en passordbehandling som administrerer brukernavn, passord og annen informasjon som er nyttig for å utføre aktiviteter på nettet.</p>	<p>1. Abbonentinformasjon, enhets- og programvaredata, inkludert: Nettlesernavn, versjon og foretrukket språk; Operativsystem, versjon eller plattform; brukerenhetens IP-adresse; *andre personopplysninger som er oppgitt av brukeren, som kan inkludere brukernavn, passord, adresser til nettsteder, fysiske adresser, kontonumre for betaling, utløpsinformasjon og annen tekst</p> <p>2. Data over tjenestebruken, inkludert: Nettstedets surfeaktivitet; søkeord på nettet; standardinnganger i forskjellige søkebokser som forvaltes av Norton-produktene; søkemotorresultater</p>	<p>1. Enhets- og programvaredata behandles av Symantec for å:</p> <ul style="list-style-type: none"> • Aktivere og optimalisere ytelsen til tjenesten; • Utføre lisensadministrasjon; • Forstå produktbruk og preferanser for å tilpasse og forbedre brukeropplevelsen; • Veilede brukeren under programvareinstallasjonen; • Levere produkt- og serviceforbedringer for å gi brukeren samt brukerens nettverk, enhet, data og identitet bed beskyttelse; og • Forbedre kundetilfredsheten fra tjenester levert via egne og tredjeparters telefonsentre. <p>2. Produktbruksdata behandles av Symantec og på vegne av Symantec for å:</p> <ul style="list-style-type: none"> • Informere brukeren om sikkerheten til nettstedet; • Blokkere nettleseing på usikre nettsteder; og • Analysere bruken av tjenesten. <p>Anonymiserte IP-adresser og informasjon om produktbruk behandles av Google Analytics' måleprotokoll for statistisk analyse og behandling av kritiske feil. Klikk her for å få informasjon om sikkerhetstiltak for data i Google Analytics.</p> <p>I tillegg kommer Symantec til å bruke aggregerte, aidentifiserte, anonymiserte eller ellers ikke-identifiserende data hentet fra innsamlede statistiske data, for å:</p> <ul style="list-style-type: none"> • Følge opp generelle undersøkelser av nettsikkerheten; • Forbedre påvisning av skadelig programvare og nett-trusler, f.eks. gjennom analyse av filprøver; • Spore og publisere rapporter om sikkerhet og risikoer/trender innen identitetstyveri; • Gjennomføre statistisk analyse av produkt plassering, inkludert analyse av trender og sammenligninger i vår aggregerte brukerbase; og • Overvåke og forbedre ytelsen til tjenesten når det gjelder tilgjengelighet og responstid.

Norton Family Premier

Produkt-/tjenestebeskrivelse	Datatilgang og -innsamling	Databehandling
<p>Norton Family Premier beskytter brukeren samt enheter som abonnenten velger å beskytte, med foreldrekontroll som er brukt gjennom abonnentsdefinerte og abonnentstyrte beskyttelsesinnstillinger og -funksjoner</p> <p>For å få mer informasjon om Norton Family Premier se avsnittet nedenfor merket «Mer informasjon om Norton Family Premier»</p>	<p>*1. Abonnementinformasjon slik som: Administratorens kontaktinformasjon inkludert, men ikke begrenset til abonnentens navn, e-postadresse og passord for å beskytte abonnentens konto; personlige data oppgitt av abonnenten under konfigurering av tjenesten eller andre etterfølgende serviceanrop;</p> <p>2. Enhets- og programvaredata, inkludert: Installasjonsstatus for Norton Family-klientprogramvaren på enheten til abonnenten eller den beskyttede brukeren; programvarekonfigurering, produktdetaljer og installasjonsstatus; lisensstatus, informasjon om lisensrettigheter, lisens-ID og lisensbruk; enhetsnavn, enhetstype, versjon av operativsystem, språk, posisjon (Global Position System, GPS), nettleserstype og versjon; enhetens maskinvare, programvare og programlager; konfigurering av program- og databasetilgang, status for krav i og overholdelse av retningslinjer, og programunntak og feillogger for arbeidsflyt;</p> <p>*3. Beskyttet brukerinformasjon som abonnenten velger å oppgi til Symantec, inkludert: Navn, kjønn, alder og fødselsår; avatarbilder, de seks siste sifrene i identifikasjonsnumrene til de beskyttede brukerne (f.eks der tilgjengelig: personnummer, nasjonalt identifikasjonsnummer), e-postadresse, mobiltelefonnummer, skolenavn og annen informasjon som abonnenten vil beskytte: innloggingsdetaljer til maskinkontoen, land og sone;</p> <p>4. Informasjon om nettverksaktiviteten til den beskyttede brukeren som abonnenten instruerer Symantec til å overvåke, inkludert per abonnentens suverene valg: Internett- og mobilenhetens aktiviteter og posisjoner; nettsted som den beskyttede brukeren prøver å besøke, og nettsteder som blokkeres av produktet; søkeord på nett som den beskyttede brukeren bruker; programmer som den beskyttede brukeren installerer eller avinstallerer på enheten, hvis abonnenten har aktivert programovervåking; den beskyttede brukerens brukstid på enheten; *den beskyttede brukerens profilnavn, profiladresse, alder, Facebook-profil-ID og besøkte videoer; beskyttede brukervisninger av videoer på YouTube.com og/eller fra Hulu, hvis abonnenten har aktivert videoovervåking.</p>	<p>1. Abonnementinformasjon behandles av Symantec for å:</p> <ul style="list-style-type: none"> • Aktivere og optimalisere ytelsen til Norton-familien; • Gi brukerstøtte eller hjelp til å feilsøke; • Sende markedsføringsinformasjon til abonnenten, i samsvar med abonnentens tillatelse eller som ellers tillatt i henhold til gjeldende lov; og • Konfigurere abonnentens Norton-konto. <p>2. Enhets- og programvaredata behandles av Symantec for å:</p> <ul style="list-style-type: none"> • Sikre produktets riktige funksjon og levere tjenestene som abonnenten krever; • Utføre lisensadministrasjon; • Evaluere og forbedre suksessraten for installering av produktet; • Forske og utvikle for å forbedre Symantecs produkter og tjenester og gi bedre beskyttelse til abonnentens og de beskyttede brukerens nettverk, enheter, data og identitet; <p>3. Informasjon om den beskyttede brukeren behandles for å:</p> <ul style="list-style-type: none"> • Identifisere og autentisere abonnenten og den beskyttede brukeren til Symantec; • Hjelp abonnenten med å oppdage eventuell misbruk av den beskyttede brukerens personlige data; og • Kommunisere med abonnenten, og på abonnentens tillatelse, med den beskyttede brukeren for å levere tjenesten. <p>4. Informasjon om aktiviteten til den beskyttede brukeren blir behandlet for å:</p> <ul style="list-style-type: none"> • Hjelp abonnenten med å overvåke aktiviteter på nettet fra den beskyttede brukerens enhet; • Begrense skaden gjort av den installerte skadelige programvaren; • Hjelp med å håndheve abonnentdefinerte regler for aktiviteter på nettet til den beskyttede brukerens enhet; • Tillate abonnenten å oppdage om den beskyttede brukeren er utsatt for trusler via nett eller SMS-/MMS-kommunikasjon; og • Hjelp abonnenten med å beskytte den beskyttede brukeren mot slike trusler. <p>I tillegg kommer Symantec til å bruke aggregerte, aidentifiserte, anonymiserte eller ellers ikke-identifiserende data hentet fra innsamlede statistiske data, for å:</p> <ul style="list-style-type: none"> • Følge opp generelle undersøkelser av nettsikkerheten; • Forbedre påvisning av skadelig programvare og nett-trusler, f.eks. gjennom analyse av filprøver; • Spore og publisere rapporter om sikkerhet og risikoer/trender innen identitetstyveri; og • Gjennomføre statistisk analyse av produktplacering, inkludert analyse av trender og sammenligninger i vår aggregerte brukerbase.

Mer informasjon om Norton Family Premier

Hvis abonnenten velger å aktivere tjenesten, tillater ikke Norton Family den beskyttede brukeren å publisere de personlige dataene sine.

Der, og i den grad det tillates ifølge lovende som gjelder i landet eller regionen der abonnenten befinner seg, kan Symantec gi en **tekstmeldingovervåkingstjeneste**, som gjør at abonnenten kan blokkere eller overvåke tekstmeldinger («SMS») og multimediemeldinger («MMS») som leveres til og fra den beskyttede brukerens mobiltelefon, samt en **tjeneste for posisjonsovervåking**. Overvåking av SMS- og MMS-utvekslinger og/eller posisjon og bruk av oversikter over slik overvåking kan være begrenset eller forbudt i henhold til lokale lover som gjelder for abonnenten. Abonnenten bør på alle måter henvende seg til lokale myndigheter før aktivering av denne funksjonen.

Når abonnenten aktiverer tjenesten for posisjonsovervåking, utfører Norton Family abonnentens instruks ved å bruke GPS for å spore og samle inn geoplasingen til den valgte mobilen abonnenten. Abonnentens samtykke og samtykke fra brukeren av mobilenheten eller samtykke fra innehaveren av foreldreansvar for en slik bruker er nødvendig for at Norton Family kan spore, samle inn, bruke eller oppgi geoplasingen til den valgte enheten. Det relevante samtykket eller samtykkene samles inn via Nortons nettportal, eller, og i tilfelle det er mulig, i produktet og bekreftes når abonnenten skriver inn betalingskortinformasjonen for å kjøpe denne tjenesten med Symantec på nett. Du kan tilbakekalle ethvert samtykke du har gitt når som helst. For å få mer informasjon om hvordan du gjør det, kan du lese «Personvernrettighetene dine»-delen av [Symantec – Global personvernerklæring for Norton](#). Etter at tjenesten er avsluttet, slettes abonnentens kontoinformasjon knyttet til denne tjenesten.

Når abonnenten har lastet ned appen på den angitte mobilenheten, kan Symantec samle inn geoplasingen til enheten, selv når appen ikke er i bruk. Vi oppgir bare informasjon om geoplasing til abonnenten, slik at abonnenten selv kan finne enheten, og vi behandler det bare for operasjonelle formål for å levere tjenestene og funksjonene etterspurt av abonnenten. Abonnenten kan ikke bruke tjenesten for posisjonsovervåking av produktet for å overvåke dataene, posisjonen, aktivitetene eller andre aspekter knyttet til andre personer enn dem abonnenten har foreldreansvar for. Abonnenter i EØS-området bør snakke med beskyttede brukere under foreldrenes ansvar, spesielt hvis de er over 13 år, og iverksette alle nødvendige tiltak for å sikre at den beskyttede brukeren forstår hva abonnentens bruk av produktet og de tilhørende tjenester medfører. Når du velger å bruke produktet og tilhørende tjenester, er abonnenten eneansvarlig for å overholde alle lover og forskrifter som gjelder for abonnentens forhold til og foreldreansvar over den beskyttede brukeren.

Overvåking av tekstmeldinger

Som standard er overvåking av tekstmeldinger slått av. Abonnenten må slå på funksjonen for overvåking av tekstmeldinger og installere Norton Family på mobilenheten som er valgt for slikt tilsyn. Når det er aktivert, samler overvåkningen av tekstmeldinger inn følgende informasjon fra den angitte enheten:

- Mobiltelefonnummeret til enheten som overvåkes og mobiltelefonnumrene til andre enheter som enheten utveksler SMS- og MMS-kommunikasjon med;
- Innholdet i SMS-meldingene som mottas eller sendes av den angitte enheten (for MMS-utvekslinger registrerer ikke Symantec innholdet i MMS-en som utveksles, bare det faktum at en MMS-utveksling skjedde);
- Hvis det er tilgjengelig, navnet på adresseboken tilknyttet den angitte enheten med mobilnummeret som sender SMS- og MMS-kommunikasjon til den angitte enheten, eller mottar slik kommunikasjon fra den;
- Datoen/klokkeslettet for samtalen;
- Geoplasingen til den valgte enheten;
- En hendelseslogg av blokkerte SMS-/MMS-meldinger, inkludert telefonnumre til partene, og tilhørende navn hvis noen er tilgjengelige i adresseboken til den angitte enheten.

Før overvåkingen av SMS- eller MMS-meldinger som en utpekt mobilenhet av abonnenten sender og/eller mottar begynner, sender Symantec et SMS-varsel til den angitte enheten og varsler brukeren av enheten om at produktet skal utføre instruksjonene til abonnent for å registrere og overvåke innholdet i SMS- eller MMS-meldingene som utveksles på den angitte enheten. Hvis, etter mottak av dette SMS-varselet, utvekslingen av SMS- eller MMS-meldinger fortsetter på den angitte enheten, starter registrering og overvåking av meldingene for formålene som beskrives i denne merknaden, i henhold til abonnentens instruksjoner. Symantec gjentar det samme SMS-varselet til den angitte enheten en gang i måneden eller hver gang det er en ny samtale.

Hvis abonnenten velger å blokkere alle SMS- eller MMS-meldinger eller meldinger med en bestemt motpart, varsler vi brukeren av den angitte enheten og sender en tekstmelding til motparten som indikerer at meldingen er blokkert og at meldingen ikke kan leveres.