Informacja o ochronie prywatności dotycząca produktów i usług Norton – *data ostatniej aktualizacji: 7 listopad 2018 r.*

Niniejszą Informację należy czytać i stosować w połączeniu z Globalnym oświadczeniem o ochronie prywatności Norton Symantec. Opisuje ona kategorie danych gromadzonych w ramach produktów i usług Norton oraz cele przetwarzania tych kategorii danych. Jej celem jest zapewnienie wymaganej przejrzystości informacji zarówno indywidualnym użytkownikom Norton jako osobom, których dane dotyczą, oraz użytkownikom ze średnich i dużych przedsiębiorstw będących administratorami danych. Należy pamiętać, że kategorie danych oznaczone gwiazdką (*) to Dane osobowe przekazywane do Symantec w celu udostępniania odpowiednich funkcji produktów i usług Norton. Wszystkie inne kategorie danych są gromadzone przez oprogramowanie Norton w celu przetwarzania w sposób nieumożliwiający ustalenia tożsamości.

Wszystkie produkty i usługi Norton są zgodne z wysokimi standardami przedstawionymi w Globalnym oświadczeniu o ochronie prywatności Norton Symantec. Ponadto, aby w sposób przejrzysty informować Państwa o unikatowych cechach i szczególnym przeznaczeniu każdego produktu i każdej usługi Norton, niniejsza Informacja, prócz opisu produktu albo usługi, zawiera opis Danych osobowych, jakie gromadzimy, oraz celów ich przetwarzania.

Jeżeli jakakolwiek część albo aspekt niniejszej Informacji jest dla Państwa nie do przyjęcia, prosimy nie pobierać, nie instalować ani nie korzystać w inny sposób z odnośnych Produktów i Usług ani ich funkcji lub prosimy także bezzwłocznie odinstalować odnośne Produkty, Usługi albo funkcje albo zaprzestać korzystania z nich. W przypadku funkcji Produktów i Usług, które wymagają podania nam przez Państwa dodatkowych Danych osobowych, albo które wymagają wyrażenia przez Państwa zgody na przetwarzanie takich Danych osobowych, gdyż jest to konieczne w celu korzystania z konkretnych funkcji dodatkowych Produktu albo Usługi, w czasie pobierania, instalacji, aktywacji albo korzystania z tej funkcji, zostaną Państwo poproszeni o ponowne zapoznanie się z niniejszą Informacją, aby mogli Państwo odpowiednio wyrazić świadomą i konkretną zgodę.

Spis treści

Norton App Lock

Opis Produktu/Usługi	Dostęp do danych i ich gromadzenie	Przetwarzanie danych
Norton App Lock umożliwia użytkownikom zabezpieczenie i ochronę aplikacji mobilnych poprzez ich zablokowanie za pomocą kodu PIN, hasła albo wzoru. Funkcję App Lock można skonfigurować w taki sposób, aby w przypadku kradzieży albo zagubienia urządzenia mobilnego przednia kamera urządzenia, o ile urządzenie ją posiada, zrobiła zdjęcie po trzech nieudanych próbach odblokowania.	*1. Adres e-mail użytkownika 2. Numery PIN i hasła do aplikacji mobilnych ustalone przez użytkownika 3. Obrazy na podstawie ustawień (zależnie od decyzji użytkownika)	1. Adres e-mail użytkownika jest zapisywany i przekazywany do spółki Symantec, aby umożliwić przetwarzanie odzyskiwania i resetowania hasła Norton App Lock. 2. 3. Wszelkie inne dane gromadzone przez urządzenie podczas ich wprowadzania przez użytkownika są przechowywane w urządzeniu użytkownika.

Norton Clean

Opis Produktu/Usługi	Dostęp do danych i ich gromadzenie	Przetwarzanie danych
Norton Clean to narzędzie do maksymalizacji pojemności pamięci, które czyści pamięć podręczną urządzenia, aby wymazać reklamy i niepożądane dane, tym samym zwalniając dodatkową pamięć.	Unikatowy identyfikator urządzenia mobilnego (IMEI)	Numer IMEI jest pobierany z urządzenia i przekazywany do spółki Symantec. Numer IMEI po przekazaniu jest natychmiast haszowany przed dalszym przetwarzaniem. Haszowanie służy monitorowaniu unikatowego użycia produktu. Po zahaszowaniu danych nie można ustalić urządzenia, z którego one pochodzą, a więc ani użytkownik, ani urządzenie nie są śledzeni ani monitorowani.

Norton Error Management

Opis Produktu/Usługi	Dostęp do danych i ich gromadzenie	Przetwarzanie danych
Norton Error Management służy do dokumentowania problemów związanych z Produktami Norton. W takim przypadku użytkownik może podjąć decyzję o zgłoszeniu błędu spółce Symantec.	1. Informacje na temat stanu komputera (język systemu, ustawienia regionalne kraju i wersja systemu operacyjnego) 2. Uruchomione procesy oraz informacje na temat ich statusu i wydajności 3. Dane z plików i folderów otwartych w czasie, gdy wystąpił błąd produktu Norton	1.-2.-3. Informacje o systemie są przetwarzane przez Symantec w celu naprawy napotkanych problemów i polepszenia wydajności Produktu Norton. W niektórych przypadkach, jeżeli błąd wystąpił z powodu zagrożenia bezpieczeństwa albo luki w zabezpieczeniach, Symantec może pozyskać i udostępnić pewne dane niezwiązane z konkretnym użytkownikiem albo nieumożliwiające jego identyfikacji partnerom w ramach szerszej społeczności cyberbezpieczeństwa, takim jak organizacje badawcze i inni dostawcy oprogramowania zabezpieczającego. Celem takiego udostępniania danych jest zwiększanie świadomości, wykrywalności i zapobieganie zagrożeniom. Symantec może także korzystać z danych statystycznych pozyskanych z takich informacji do śledzenia tendencji związanych z zagrożeniami bezpieczeństwa i publikowania raportów na ten temat.

Norton Community Watch

Opis Produktu/Usługi	Dostęp do danych i ich gromadzenie	Przetwarzanie danych
Norton Community Watch umożliwia użytkownikom produktów zabezpieczających Norton pomagać w polepszaniu rozpoznawania nowych zagrożeń dla bezpieczeństwa i skracaniu czasu zapewnienia przed nimi ochrony. Program zbiera wybrane dane dotyczące bezpieczeństwa i aplikacji, a następnie wysyła je do Symantec celem analizy, aby wykrywać nowe zagrożenia i ich źródła. Program ten pozwala stworzyć lepszy, silniejszy produkt zabezpieczający dzięki analizie danych przesłanych od użytkownika. Włączając się w program Norton Community Watch: 1. Uczestniczą Państwo w budowaniu lepszej, pełniejszej wiedzy na temat zagrożeń w cyberprzestrzeni i ochrony przed nimi dzięki danym przesyłanym przez Państwa i innych uczestników. W naszej wewnętrznej technologii wykorzystujemy zaawansowane algorytmy służące obliczaniu wskaźnika oceny bezpieczeństwa każdego pliku pobranego, zainstalowanego albo uruchomionego na Państwa urządzeniu, jednakże bez wskazywania w jakikolwiek sposób na Państwa albo kogokolwiek innego osobiście. Użytkownicy produktów zabezpieczających Norton odnoszą korzyści płynące z tej innowacyjnej technologii, gdy produkt Norton: *a. blokuje pobieranie szkodliwych plików za pomocą Download Insight. Norton mówi użytkownikowi, czy dane pobieranie uznawane jest za bezpieczne, niebezpieczne, albo że jego profil bezpieczeństwa jest nieznany. Jeżeli pobieranie nie jest bezpieczne, nasze produkty podejmują natychmiastowe działania mające na celu ochronę użytkownika; b. osiąga lepsze wyniki wykrywania i zmniejsza liczbę fałszywych alarmów; *c. wykonuje szybsze skanowanie za pomocą Norton Insight zatwierdzając szybciej pliki, które zostały przesłane, przeanalizowane i zatwierdzone jako bezpieczne przez Norton Community Watch. 2. Udostępniając kluczowe dane dotyczące bezpieczeństwa i aplikacji wnoszą Państwo swój wkład w wiedzę niezbędną do rozpoznawania nowych zagrożeń i blokowania ich zanim dojdzie do ich rozprzestrzenienia. * Program Norton Insight jest dostępny tylko w systemie operacyjnym Windows.	1. Identyfikator urządzenia (dane generowane przez Symantec) 2. Numer seryjny produktu (dane przypisane produktowi przez Symantec) 3. Numer konta Norton (Norton Account Number) (dane generowane przez Symantec) *4. Ścieżki plików *5. Pliki niewykonywalne i przenośne pliki wykonywalne uznane za oprogramowanie złośliwe 6. Adresy URL odwiedzanych witryn, które produkt Norton uznaje za potencjalnie wykorzystywane do oszustwa 7. Adres URL witryny, którą użytkownik odwiedził tuż przed zainstalowaniem na komputerze pobranego zagrożenia bezpieczeństwa 8. Informacje na temat procesów i aplikacji uruchamianych na urządzeniu użytkownika od czasu do czasu, w tym w czasie, w którym wystąpiło potencjalne zagrożenie bezpieczeństwa 9. Próbka danych przesłanych przez urządzenie użytkownika w odpowiedzi na potencjalne zagrożenie bezpieczeństwa	Norton Community Watch jest usługą obsługiwaną i zarządzaną przez Symantec wewnętrznie, dlatego wszelkie zgromadzone dane są przekazywane do Symantec w następujący sposób: 1. Identyfikator urządzenia jest konieczny do kontrolowania liczby unikatowych urządzeń korzystających z produktu w ramach każdej subskrypcji, a także do kontrolowania i egzekwowania praw licencyjnych i upoważnień. 2. Numer seryjny produktu przyznawany jest każdemu użytkownikowi i służy zagwarantowaniu, by każdy produkt miał licencję Symantec na użytkowanie. 3. Numer konta Norton (Norton Account Number) jest potrzebny do kontrolowania liczby użytkowników objętych subskrypcją poszczególnych produktów Norton. 4.-5. Ścieżki plików oraz pliki niewykonywalne i przenośne pliki wykonywalne są rejestrowane, aby pomóc ustalić źródło i lokalizację logiczną zagrożeń dla cyberbezpieczeństwa wpływających na urządzenie użytkownika albo pochodzących z niego. 6.-7. Adresy URL służą identyfikacji internetowych źródeł potencjalnych zagrożeń bezpieczeństwa oraz poprawie zdolności Produktów i Usług Symantec do wykrywania złośliwych działań, szkodliwych zdarzeń, witryn wykorzystywanych do oszustw, oprogramowania przestępczego oraz innych form zagrożenia bezpieczeństwa w Internecie. 8.-9. Dane urządzenia wykorzystywane są do polepszenia wiedzy Symantec na temat zagrożeń dla cyberbezpieczeństwa i ich rozumienia. Dane urządzenia są także przetwarzane w celu zapewnienia lepszej ochrony użytkowników Produktów i Usług Symantec w przyszłości, a także na potrzeby statystycznych analiz tendencji w dziedzinie zagrożeń dla cyberbezpieczeństwa.

Norton Core

Opis Produktu/Usługi	Dostęp do danych i ich gromadzenie	Przetwarzanie danych
Norton Core to router bezprzewodowy zapewniający ochronę przeciwko złośliwemu oprogramowaniu, wirusom, hakerom i innym zagrożeniom dla cyberbezpieczeństwa urządzeniom połączonym z routerem.	*1. Sieć bezprzewodowa SSID/hasło (zaszyfrowana) 2. Informacje na temat urządzenia, w tym wszelkie Dane osobowe użyte przez użytkownika podczas nadawania nazw urządzeniom, oraz, o ile podane przez użytkownika, imię albo pseudonim osoby, do której urządzenie jest przypisane, oraz dane agenta użytkownika urządzenia/aplikacji, w tym rodzaj, producent i model urządzenia, system operacyjny i adres IP 3. Dane dotyczące wykorzystania urządzenia, w tym dane dotyczące czasu ostatniego korzystania z urządzenia, czasu korzystania z Internetu przez każde z podłączonych urządzeń, oraz dzienniki bram połączeń internetowych 4. Informacje na temat kontroli rodzicielskiej i jej ustawienia, określone i skonfigurowane przez użytkownika, w tym zablokowane witryny, odwiedzane witryny oraz informacje dotyczące filtra czasu i treści, a także adresy URL witryn określonych jako niebezpieczne albo potencjalnie niebezpieczne *5. Dane osobowe, które użytkownik mógł podać tworząc Konto Norton, w tym nazwa użytkownika i nieobowiązkowe zdjęcie *6. Dane osobowe podane przez użytkownika działowi wsparcia technicznego i wsparcia łączności, takie jak identyfikator użytkownika, imię i nazwisko, stanowisko, zasady dotyczące użytkowników oraz informacje o urządzeniu 7. Dane telemetryczne dotyczące zagrożeń dla cyberbezpieczeństwa, w tym dzienniki prób pobrania złośliwych plików wykonywalnych/aplikacji mobilnych, zapis innych zdarzeń albo czynności obarczonych	1. Informacje na temat sieci bezprzewodowych są przetwarzane w związku z konfiguracją sieci Wi-Fi określoną przez użytkownika. 2. Informacje na temat urządzenia są przetwarzane w celu zarządzania licencjami, analizy urządzeń i ruchu w celu monitorowania sprawności i łączności routera oraz pomocy w jego debugowaniu, w celu poznania użytkowania produktu i reagowania na ostrzeżenia. 3. Dane na temat wykorzystania urządzenia są przetwarzane w celu: • optymalizacji działania Norton Core; • informowania użytkowników o bezpieczeństwie witryn internetowych; oraz • blokowania przeglądania niebezpiecznych witryn. 4. Informacje na temat kontroli rodzicielskiej i jej ustawienia służą egzekwowaniu zasad i polityk ustalonych przez użytkownika wobec profili objętych kontrolą, pomocy w wykrywaniu przez użytkownika wszelkich przypadków niewłaściwego wykorzystania Danych osobowych powiązanych z tymi profilami oraz komunikowaniu się z użytkownikiem i profilami objętymi kontrolą. 5.-6. Informacje dotyczące konta użytkownika są gromadzone przez Symantec w celu świadczenia usług ujętych w umowie z klientem i zapewniania wsparcia technicznego. 7. Dane telemetryczne dotyczące zagrożeń dla cyberbezpieczeństwa są przesyłane do Symantec na potrzeby badań i rozwoju, których celem jest ulepszanie produktów i usług Symantec i lepsza ochrona sieci, urządzeń, danych i tożsamości użytkowników. 8. Informacje kontaktowe użytkownika i preferencje są przekazywane do Symantec w celu: • przeprowadzania użytkownika przez proces instalacji urządzenia Norton Core; • informowania użytkownika o sposobach na zwiększenie komfortu użytkowania; • dostosowania informacji prezentowanych użytkownikowi na podstawie jego preferencji (takich jak język i region); oraz • zwiększania zadowolenia klientów ze świadczonych usług za pośrednictwem własnych i zewnętrznych centrów obsługi telefonicznej. 9. Adresy wysyłki i informacje powiązane są przetwarzane w celu dostarczenia użytkownikowi sprzętu Norton Core. 10. Szczegółowe informacje dotyczące Norton Community Watch można znaleźć w rozdziale Norton Community Watch niniejszej Informacji. Prócz tego Symantec będzie wykorzystywać zagregowane, pozbawione elementów identyfikacyjnych, zanonimizowane albo w inny sposób uniemożliwiające identyfikację użytkownika dane pozyskane ze zgromadzonych danych, takich jak dane statystyczne, do następujących celów: • prowadzenie ogólnych badań w obszarze cyberbezpieczeństwa; • zwiększanie wykrywalności złośliwego oprogramowania i zagrożeń dla cyberbezpieczeństwa, np. poprzez analizę próbek plików;

	ryzykiem, a także artefakty, takie jak próbki złośliwego oprogramowania *8. Dane kontaktowe użytkownika, wyrażone preferencje *9. Adresy do wysyłki i informacje powiązane 10. Norton Core umożliwia udział w programie Norton Community Watch	• monitorowanie i publikowanie raportów na temat bezpieczeństwa i tendencji oraz zagrożeń związanych z kradzieżą tożsamości; • prowadzenie analiz statystycznych zastosowania produktów, w tym analizy tendencji i porównań w zagregowanych bazach użytkowników; • monitorowanie i podnoszenie wydajności produktów pod względem ich dostępności i szybkości działania; • poznanie częstości komunikacji związanej z produktami w celu optymalizacji ogólnego komfortu użytkownika; oraz • zdobywanie innych informacji biznesowych i rynkowych niezwiązanych z konkretnymi użytkownikami w celu podnoszenia wydajności naszych działań.

Norton Mobile Security

Opis Produktu/Usługi	Dostęp do danych i ich gromadzenie	Przetwarzanie danych
Norton Mobile Security zapewnia chronionym użytkownikom oraz tym urządzeniom, które subskrybent zdecyduje się chronić, ochronę smartfonów i tabletów przeciwko zagrożeniom cyfrowym, odzyskiwanie zgubionych albo skradzionych urządzeń oraz odzyskiwanie danych kontaktowych	1. Dane urządzeń mobilnych chronionych użytkowników, w tym identyfikatory sprzętu (nr IMEI, adres MAC Wi-Fi, identyfikator UDID), informacje dotyczące subskrybenta, numer telefonu komórkowego oraz inne chronione dane kontaktowe użytkownika, nazwa/rodzaj oraz producent urządzenia, rodzaj i wersja systemu operacyjnego, operator sieci bezprzewodowej, rodzaj sieci, kraj pochodzenia, identyfikator zgłoszenia, certyfikaty zainstalowane przez użytkownika, nazwa domeny internetowej i powiązany łańcuch certyfikatów SSL z urządzenia oraz adres IP 2. Dane dotyczące użycia, takie jak informacje na temat pobierania i częstości używania, dane z dzienników i pliki cookie, a także informacje na temat usług sieciowych dotyczące tego, jak użytkownik łączy się z usługami sieciowymi 3. Nazwy plików i aplikacji na urządzeniu użytkownika za każdym razem, gdy Produkt wykonuje skanowanie, w tym przeskanowanych aplikacji, które nie znajdują się obecnie w bazie znanych aplikacji Symantec,	1. Dane dotyczące urządzenia mobilnego, informacje na temat subskrybenta i chronione informacje kontaktowe użytkownika są przetwarzane w celu: • umożliwienia działania Produktu i jego optymalizacji; • uwierzytelniania tożsamości chronionego użytkownika na potrzeby Symantec; • przeprowadzania użytkownika przez proces instalacji; • komunikacji z chronionym użytkownikiem w celu świadczenia usługi; • zarządzania licencjami; oraz • zwiększania zadowolenia klientów ze świadczonych usług za pośrednictwem własnych i zewnętrznych centrów obsługi telefonicznej. 2. Dane dotyczące użycia są przetwarzane w celu: poznania sposobu i preferencji użycia produktu w celu jego personalizacji i zwiększenia komfortu użytkownika. 3. Nazwy plików i aplikacji, zawartość Kalendarza (np. adresy URL w zaproszeniach) i zawartość karty SD są przetwarzane w celu: • ostrzegania użytkownika przed aplikacjami potencjalnie niebezpiecznymi; • skanowania urządzenia pod kątem złośliwego oprogramowania; oraz • usuwania osobistych treści z urządzenia, jeśli użytkownik postanowi włączyć i wykonać polecenie Wipe dostępne w ramach Produktu. 4. Dane przeglądania są przetwarzane w celu: • informowania użytkowników o bezpieczeństwie witryn internetowych; • blokowania przeglądania niebezpiecznych witryn; oraz • usuwania historii przeglądania i zakładek, jeśli użytkownik postanowi użyć funkcji Web Protection albo polecenia Wipe dostępnych w ramach Produktu. 5. Dane kontaktowe, w tym rejestry połączeń i SMS-ów na urządzeniu użytkownika są przetwarzane w celu umożliwienia działania funkcji blokowania połączeń/wiadomości tekstowych, jeśli użytkownik postanowi z nich korzystać.

	aby chronić użytkownika przez złośliwym oprogramowaniem albo niebezpiecznymi funkcjami, a także zawartość Kalendarza i karty SD, o ile dostępne 4. Adresy URL odwiedzanych stron, historia i zakładki *5. Zależnie od decyzji użytkownika lista kontaktów na urządzeniu użytkownika wraz z rejestrem połączeń i SMS-ów 6. Ustawienia dźwięku połączeń i urządzenia *7. Dane dotyczące lokalizacji urządzenia *8. Produkt można także skonfigurować w taki sposób, o ile pozwala na to wyposażenie i gdy zgłoszono zagubienie albo kradzież urządzenia, aby przednia kamera urządzenia zrobiła zdjęcie, jeśli urządzenie jest nadal używane, jeśli wprowadzono nieprawidłowe hasło po jednej nieudanej próbie odblokowania urządzenia albo jeśli urządzenie wyłączono, a następnie włączono 9. Kopia zapasowa danych z urządzenia mobilnego, w tym lista kontaktów, historia połączeń, telefony i wiadomości tekstowe	6. Ustawienia telefonu są wykorzystywane do blokowania połączeń przychodzących od osób z listy kontaktów albo w celu modyfikacji ustawień dźwiękowych, jeśli użytkownik postanowi włączyć i zastosować funkcję blokowania lub polecenie Scream dostępne w ramach Produktu. 7. 8. Lokalizacja urządzenia i dane zdjęć mogą być gromadzone i chronione na życzenie użytkownika, aby ustalić położenie urządzenia w przypadku jego zagubienia albo kradzieży. Produkt może także umożliwić subskrybentowi zdalne wykonywanie poleceń, aby ułatwić ustalenie położenia chronionego urządzenia użytkownika w przypadku jego zagubienia albo kradzieży. W niektórych przypadkach, gdy zgłoszono zagubienie albo kradzież urządzenia, urządzenie to może zostać zdalnie zablokowane. W przypadku zgłoszenia zagubienia albo kradzieży urządzenia, produkt może zostać w dowolnym momencie wyłączony. Za zgodą chronionego użytkownika możliwe jest przechowanie historii dziesięciu ostatnich znanych lokalizacji urządzenia, aby umożliwić chronionemu użytkownikowi śledzenie niedawnych ruchów urządzenia nawet jeśli urządzenie nie jest aktualnie w użyciu. 9. Dane kopii zapasowej są przechowywane w celu zapewnienia działania funkcji Produktu związanych z tworzeniem kopii zapasowych i odzyskiwaniem, o ile użytkownik zdecyduje się z nich skorzystać. Prócz tego Symantec będzie wykorzystywać zagregowane, pozbawione elementów identyfikacyjnych, zanonimizowane albo w inny sposób uniemożliwiające identyfikację użytkownika dane pozyskane ze zgromadzonych danych, takich jak dane statystyczne, do następujących celów: • prowadzenie ogólnych badań w obszarze cyberbezpieczeństwa; • zwiększanie wykrywalności złośliwego oprogramowania i zagrożeń dla cyberbezpieczeństwa, np. poprzez analizę próbek plików; • monitorowanie i publikowanie raportów na temat bezpieczeństwa i tendencji oraz zagrożeń związanych z kradzieżą tożsamości; • prowadzenie analiz statystycznych zastosowania produktów, w tym analizy tendencji i porównań w zagregowanych bazach użytkowników; • monitorowanie i podnoszenie wydajności produktów pod względem ich dostępności i szybkości działania; • poznanie częstości komunikacji związanej z produktami w celu optymalizacji ogólnego komfortu użytkownika; oraz • zdobywanie innych informacji biznesowych i rynkowych niezwiązanych z konkretnymi użytkownikami w celu podnoszenia wydajności naszych działań.

Norton Security Scan

Opis Produktu/Usługi	Dostęp do danych i ich gromadzenie	Przetwarzanie danych
Norton Security Scan umożliwia skanowanie wybranych przez użytkownika urządzeń końcowych, wykrywa potencjalne problemy i zagrożenia oraz przedstawia użytkownikowi	1. Identyfikator urządzenia (dane wygenerowane wewnętrznie przez Symantec); funkcja instalowania/odinstalowywania w urządzeniu; informacje na temat urządzenia i dane agenta	1. Identyfikator urządzenia i informacje powiązane są wykorzystywane przez Symantec w celu: • przeprowadzania użytkownika przez proces instalacji; • komunikacji z użytkownikiem w celu świadczenia usługi; • poznania sposobu i preferencji użycia usługi w celu jej personalizacji i zwiększenia komfortu użytkownika. 2. Informacje telemetryczne są wykorzystywane przez Symantec w celu:

zalecane produkty i rozwiązania.	użytkownika urządzenia/aplikacji, w tym rodzaj urządzenia, wersja i język systemu operacyjnego, producent i model; system operacyjny; oraz powiązane informacje geograficzne 2. Informacje telemetryczne dotyczące przeskanowanych plików, komfortu użytkownika oraz zagrożeń wykrytych, naprawionych i pozostałych; data i czas skanowania po zgłoszeniu; informacje na temat stanu dotyczące instalacji i działania, które mogą przypadkowo obejmować Dane osobowe, jeżeli zawiera je ścieżka pliku albo nazwa folderu	• umożliwienia działania Usługi i jej optymalizacji; oraz • na potrzeby badań i rozwoju, których celem jest ulepszanie produktów i usług Symantec i lepsza ochrona sieci, urządzeń, danych i tożsamości użytkowników. Prócz tego Symantec będzie wykorzystywać zagregowane, pozbawione elementów identyfikacyjnych, zanonimizowane albo w inny sposób uniemożliwiające identyfikację użytkownika dane pozyskane ze zgromadzonych danych, takich jak dane statystyczne, do następujących celów: • prowadzenie ogólnych badań w obszarze cyberbezpieczeństwa; • zwiększanie wykrywalności złośliwego oprogramowania i zagrożeń dla cyberbezpieczeństwa, np. poprzez analizę próbek plików; • monitorowanie i publikowanie raportów na temat bezpieczeństwa i tendencji oraz zagrożeń związanych z kradzieżą tożsamości; • prowadzenie analiz statystycznych zastosowania produktów, w tym analizy tendencji i porównań w zagregowanych bazach użytkowników; • monitorowanie i podnoszenie wydajności produktów pod względem ich dostępności i szybkości działania; • poznanie częstości komunikacji związanej z produktami w celu optymalizacji ogólnego komfortu użytkownika; oraz • zdobywanie innych informacji biznesowych i rynkowych niezwiązanych z konkretnymi użytkownikami w celu podnoszenia wydajności naszych działań.

Norton Secure Login

Opis Produktu/Usługi	Dostęp do danych i ich gromadzenie	Przetwarzanie danych
Norton Secure Login (NSL) to funkcja dostawcy tożsamości zapewniająca proste, bezpieczne i scentralizowane uwierzytelnianie użytkowników. Symantec udostępnia infrastrukturę zarządzania tożsamością milionom użytkowników różnych produktów Norton.	*1. Dane osobowe ułatwiające uwierzytelnienie tożsamości użytkownika, takie jak adres zamieszkania, numer telefonu, data urodzenia lub numer karty kredytowej; dane kontaktowe użytkownika; wszelkie inne Dane osobowe, które użytkownik doda do swojego Konta Norton albo poda w celu uzyskania wsparcia technicznego albo wsparcia łączności, takie jak imię i nazwisko oraz dane dotyczące urządzenia 2. Informacje dotyczące urządzenia, produktów i usług oraz dane agenta użytkownika urządzenia/aplikacji, w tym rodzaj urządzenia; producent; model; system operacyjny i jego wersja; informacje o urządzeniu; dane dotyczące czasu pracy i wydajności; zainstalowane aplikacje; powiązane informacje geograficzne; adres MAC oraz adres IP 3. Dane użycia dotyczące korzystania z Internetu, takie jak adresy URL i adresy IP odwiedzanych witryn internetowych, wyszukiwane słowa kluczowe i wyniki wyszukiwania, a także informacje dotyczące potencjalnych zagrożeń bezpieczeństwa (w tym informacje dotyczące adresów URL i adresów IP witryn uznanych za potencjalnie wykorzystywane do oszustwa mogące zawierać Dane osobowe, które dana witryna próbuje uzyskać bez zgody użytkownika)	1. Dane osobowe są przetwarzane przez Symantec w celu: • uwierzytelniania tożsamości użytkownika na potrzeby Symantec albo innych podmiotów zewnętrznych, które korzystają z funkcji Norton Security Login; • wystawiania poświadczenia tożsamości lub zapobiegania fałszywym transakcjom realizowanym w imieniu użytkownika; • przeprowadzania użytkownika przez proces konfiguracji; • komunikacji z użytkownikiem w celu świadczenia usługi, w tym udzielania wsparcia; oraz • zwiększania zadowolenia klientów ze świadczonych usług za pośrednictwem własnych i zewnętrznych centrów obsługi telefonicznej. 2. Informacje dotyczące urządzenia, produktów i usług są przetwarzane przez Symantec w celu: • umożliwienia działania Produktów i Usług oraz ich optymalizacji; • zarządzania licencjami; oraz • poznania sposobu i preferencji użycia produktu w celu jego personalizacji i zwiększenia komfortu użytkownika. 3. Dane dotyczące użycia są przetwarzane przez Symantec w celu: • informowania użytkowników o bezpieczeństwie witryn internetowych; • blokowania przeglądania niebezpiecznych witryn; oraz • na potrzeby badań i rozwoju, których celem jest ulepszanie produktów i usług Symantec i lepsza ochrona sieci, urządzeń, danych i tożsamości użytkowników. Prócz tego Symantec będzie wykorzystywać zagregowane, pozbawione elementów identyfikacyjnych, zanonimizowane albo w inny sposób uniemożliwiające identyfikację użytkownika dane pozyskane ze zgromadzonych danych, takich jak dane statystyczne, do następujących celów: • prowadzenie ogólnych badań w obszarze cyberbezpieczeństwa; • zwiększanie wykrywalności złośliwego oprogramowania i zagrożeń dla cyberbezpieczeństwa, np. poprzez analizę próbek plików; • monitorowanie i publikowanie raportów na temat bezpieczeństwa i tendencji oraz zagrożeń związanych z kradzieżą tożsamości; • prowadzenie analiz statystycznych zastosowania produktów, w tym analizy tendencji i porównań w zagregowanych bazach użytkowników; • monitorowanie i podnoszenie wydajności produktów pod względem ich dostępności i szybkości działania; • poznanie częstości komunikacji związanej z produktami w celu optymalizacji ogólnego komfortu użytkownika; oraz • zdobywanie innych informacji biznesowych i rynkowych niezwiązanych z konkretnymi użytkownikami w celu podnoszenia wydajności naszych działań.

Usługi Norton Ultimate Help Desk oraz Norton Computer Tune-Up

Opis Produktu/Usługi	Dostęp do danych i ich gromadzenie	Przetwarzanie danych
Usługa Ultimate Help Desk umożliwia użytkownikowi kontakt z ekspertem w celu uzyskania wsparcia w kwestiach technicznych od konfiguracji sieci po diagnostykę urządzeń i rozwiązywanie problemów. Norton Computer Tune-Up to funkcja będąca częścią usługi Norton Ultimate Help Desk, z pomocą której urządzenie użytkownika może działać jak nowe dzięki diagnostyce.	*1. Informacje związane ze zgłoszeniem podawane przez użytkownika agentom usług Symantec przez telefon albo wprowadzane za pośrednictwem interfejsu Symantec online podczas dokonywania zgłoszenia dotyczącego Usług Norton 2. Informacje o systemie, w tym: typ i wersja systemu operacyjnego i przeglądarki używanych na urządzeniu; czy włączona jest zapora ogniowa; czy zainstalowano oprogramowanie antywirusowe oraz czy jest ono uruchomione i aktualne; pojemność i wolna przestrzeń pamięci; konfiguracja proxy oraz lista ścieżek narzędzia Support Software Tool; informacje o przeglądarce, w tym dotyczące bezpieczeństwa i ustawień plików tymczasowych; aktywne porty, plik hosts i ustawienia interfejsu sieciowego urządzenia; informacje na temat zainstalowanych programów i aktywnych procesów; informacje z pliku dziennika aplikacji i systemu operacyjnego oraz dane rejestru 3. Informacje diagnostyczne, w tym: liczba przeskanowanych plików, zagrożeń wykrytych i naprawionych przez Support Software Tool; rodzaj wykrytych zagrożeń; poziom bezpieczeństwa (dobry/umiarkowany/niski) urządzenia określony przez Support Software Tool; liczba i rodzaj pozostałych zagrożeń, które nie zostały naprawione przez Support Software Tool	1. Informacje dotyczące zgłoszenia są przetwarzane przez Symantec w celu: • komunikacji z użytkownikiem w celu świadczenia usługi; • poznania sposobu i preferencji użycia produktu w celu jego personalizacji i zwiększenia komfortu użytkownika; oraz • zwiększania zadowolenia klientów ze świadczonych usług za pośrednictwem własnych i zewnętrznych centrów obsługi telefonicznej. 2. Informacje o systemie są przetwarzane przez Symantec w celu: • świadczenia Usług zamówionych przez użytkownika; • umożliwienia działania Usług i ich optymalizacji; oraz • przeprowadzania użytkownika przez proces konfiguracji. 3. Informacje diagnostyczne są przetwarzane przez Symantec w celu: • informowania użytkownika o rezultacie wykonanych usług; oraz • na potrzeby badań i rozwoju, których celem jest ulepszanie produktów i usług Symantec i lepsza ochrona sieci, urządzeń, danych i tożsamości użytkowników. Prócz tego Symantec będzie wykorzystywać zagregowane, pozbawione elementów identyfikacyjnych, zanonimizowane albo w inny sposób uniemożliwiające identyfikację użytkownika dane pozyskane ze zgromadzonych danych, takich jak dane statystyczne, do następujących celów: • prowadzenie ogólnych badań w obszarze cyberbezpieczeństwa; • zwiększanie wykrywalności złośliwego oprogramowania i zagrożeń dla cyberbezpieczeństwa, np. poprzez analizę próbek plików; • monitorowanie i publikowanie raportów na temat bezpieczeństwa i tendencji oraz zagrożeń związanych z kradzieżą tożsamości; • prowadzenie analiz statystycznych zastosowania produktów, w tym analizy tendencji i porównań w zagregowanych bazach użytkowników; • monitorowanie i podnoszenie wydajności produktów pod względem ich dostępności i szybkości działania; • poznanie częstości komunikacji związanej z produktami w celu optymalizacji ogólnego komfortu użytkownika; oraz • zdobywanie innych informacji biznesowych i rynkowych niezwiązanych z konkretnymi użytkownikami w celu podnoszenia wydajności naszych działań.

Norton Secure VPN (dawniej Norton WiFi Privacy)

Opis Produktu/Usługi	Dostęp do danych i ich gromadzenie	Przetwarzanie danych
Norton Secure VPN chroni urządzenia użytkownika i zabezpiecza dane użytkownika szyfrując jego informacje w obrębie każdego połączenia internetowego i zachowując prywatność użytkownika.	1. Informacje na temat subskrybenta i dane dotyczące urządzenia, w tym nazwa urządzenia, rodzaj, wersja systemu operacyjnego i język; 2. Łączne wykorzystanie przepustowości; 3. Dane na temat chwilowego użycia w celu wsparcia usunięcia problemu związanego z usługą.	1. Symantec przetwarza informacje na temat subskrybenta i dane dotyczące urządzenia mobilnego w celu: • umożliwienia działania Usług i ich optymalizacji; • poznania sposobu i preferencji użycia produktu w celu jego personalizacji i zwiększenia komfortu użytkownika; • przeprowadzania użytkownika przez proces instalacji oprogramowania i korzystania z Usługi; • komunikacji z użytkownikiem w celu świadczenia usługi; • przypominania użytkownikowi o konieczności chronienia przesyłanych informacji; oraz • zwiększania zadowolenia klientów ze świadczonych usług za pośrednictwem własnych i zewnętrznych centrów obsługi telefonicznej. 2. Dane dotyczące wykorzystania przepustowości są przetwarzane przez Symantec w celu naliczania opłat, dokonywania operacji sieciowych i udzielania wsparcia. 3. Dane dotyczące chwilowego użycia są przetwarzane przez Symantec w celu: • doboru najbardziej odpowiedniego serwera, z którym ma zostać nawiązane połączenie; oraz • na potrzeby badań i rozwoju, których celem jest ulepszanie produktów i usług Symantec i lepsza ochrona sieci, urządzeń, danych i tożsamości użytkowników. Podczas użytkowania Norton Secure VPN przekierowujemy ruch internetowy użytkownika poprzez sieć Symantec, w której nie są tworzone dzienniki aktywności. Oznacza to, że Symantec nie przechowuje źródłowych adresów IP użytkowników gdy są oni połączeni z Norton Secure VPN i z tego powodu Symantec nie może ustalić tożsamości poszczególnych osób. Automatyczne zarządzanie ruchem Symantec oparte na regułach może wymagać analizowania ruchu danych w Internecie w czasie rzeczywistym, w tym witryn docelowych albo adresów IP i źródłowych adresów IP, choć nie jest tworzony dziennik dotyczący tych informacji. Symantec nie przechowuje informacji o aplikacjach, usługach ani witrynach internetowych, które użytkownik pobiera, wykorzystuje albo odwiedza. Ponieważ Symantec zarządza siecią globalną, ruch w Internecie użytkownika może być przekierowywany przez jedno albo więcej różnych państw, co wyjaśniono w Globalnym oświadczeniu o ochronie prywatności Norton Symantec. Prócz tego Symantec będzie wykorzystywać zagregowane, pozbawione elementów identyfikacyjnych, zanonimizowane albo w inny sposób uniemożliwiające identyfikację użytkownika dane pozyskane ze zgromadzonych danych, takich jak dane statystyczne, do następujących celów: • prowadzenie ogólnych badań w obszarze cyberbezpieczeństwa; • zwiększanie wykrywalności złośliwego oprogramowania i zagrożeń dla cyberbezpieczeństwa, np. poprzez analizę próbek plików; • monitorowanie i publikowanie raportów na temat bezpieczeństwa i tendencji oraz zagrożeń związanych z kradzieżą tożsamości; • prowadzenie analiz statystycznych zastosowania produktów, w tym analizy tendencji i porównań w zagregowanych bazach użytkowników; • monitorowanie i podnoszenie wydajności produktów pod względem ich dostępności i szybkości działania; • poznanie częstości komunikacji związanej z produktami w celu optymalizacji ogólnego komfortu użytkownika; oraz • zdobywanie innych informacji biznesowych i rynkowych niezwiązanych z konkretnymi użytkownikami w celu podnoszenia wydajności naszych działań.

Produkty zabezpieczające Norton (Security, Internet Security, One, Antivirus i 360)

Niniejszy rozdział poświęcony jest produktom Norton Security (Standard, Deluxe i Premium), Norton Internet Security, Norton One, Norton Antivirus, Norton Antivirus Basic, Norton 360, Norton 360PE i Norton 360MD.

Opis Produktu/Usługi	Dostęp do danych i ich gromadzenie	Przetwarzanie danych
Produkty Norton Security zapewniają bezpieczeństwo komputera użytkownika końcowego i ochronę przed oprogramowaniem wymuszającym okup, wirusami, oprogramowaniem szpiegującym, złośliwym oprogramowaniem i innymi zagrożeniami w Internecie.	1. Informacje na temat subskrybenta i dane dotyczące urządzenia, w tym *Dane osobowe, które użytkownik mógł wprowadzić tworząc Konto Norton, takie jak nazwa użytkownika i nieobowiązkowe zdjęcie; wszelkie *Dane osobowe użyte przez użytkownika podczas nadawania nazw urządzeniom oraz ewentualnie imię albo pseudonim osoby, do której urządzenie jest przypisane, a także dane agenta użytkownika urządzenia/aplikacji, w tym rodzaj, producent i model urządzenia; system operacyjny i jego wersja; aplikacje i ich wersje; powiązane informacje geograficzne, adres MAC, Identyfikator urządzenia i adres IP; informacje dotyczące statusu instalacji i działania, które mogą przypadkowo obejmować Dane osobowe, jeżeli zawiera je nazwa pliku albo folderu; wszelkie Dane osobowe podane przez użytkownika działowi wsparcia technicznego albo wsparcia łączności Symantec, takie jak identyfikator użytkownika, imię i nazwisko, stanowisko, polityki oraz informacje o urządzeniu 2. Dane dotyczące korzystania z Internetu, takie jak adresy URL i adresy IP odwiedzanych witryn internetowych, wyszukiwane słowa kluczowe i wyniki wyszukiwania, a także informacje dotyczące potencjalnych zagrożeń bezpieczeństwa (w tym informacje dotyczące adresów URL i adresów IP witryn uznanych za potencjalnie wykorzystywane do oszustwa, mogące zawierać Dane osobowe, które dana witryna próbuje uzyskać bez zgody użytkownika) 3. Dane dotyczące wykorzystania i diagnostyki urządzenia, w tym: dane dotyczące czasu ostatniego korzystania z urządzenia, czasu korzystania z Internetu przez każde z podłączonych urządzeń oraz dzienniki bram zawierające szczegółowe informacje na temat aktywności połączenia sieciowego; pliki wykonywalne zidentyfikowane jako potencjalne złośliwe oprogramowanie, które mogą obejmować Dane osobowe pozyskane przez to złośliwe oprogramowanie bez zgody użytkownika; wiadomości e-mail przesłane do Symantec za zgodą użytkownika zgłoszone jako spam albo nieprawidłowo zidentyfikowane jako spam; informacje dotyczące „zrzutu awaryjnego” albo informacje zawarte w raporcie, który użytkownik może dobrowolnie	1. Symantec przetwarza informacje na temat subskrybenta i dane dotyczące urządzenia w celu: • umożliwienia działania Produktów i Usług oraz ich optymalizacji; • uwierzytelniania tożsamości użytkownika na potrzeby Symantec; • poznania sposobu i preferencji użycia produktu w celu jego personalizacji i zwiększenia komfortu użytkownika; • przeprowadzania użytkownika przez proces instalacji; • komunikacji z użytkownikiem w celu świadczenia usługi; • zarządzania licencjami; oraz • zwiększania zadowolenia klientów ze świadczonych usług za pośrednictwem własnych i zewnętrznych centrów obsługi telefonicznej. 2. Dane dotyczące korzystania z Internetu są przetwarzane w celu: • informowania użytkownika o bezpieczeństwie witryn internetowych; oraz • blokowania przeglądania niebezpiecznych witryn. 3. Symantec przetwarza dane dotyczące wykorzystania i diagnostyki urządzenia w celu: • poznania sposobu użycia produktu; • zapewniania funkcji zabezpieczających Produktów i Usług; oraz • na potrzeby badań i rozwoju, których celem jest ulepszanie produktów i usług Symantec i lepsza ochrona sieci, urządzeń, danych i tożsamości użytkowników. 4. Informacje na temat kontroli rodzicielskiej i jej ustawienia służą egzekwowaniu zasad i polityk ustalonych przez użytkownika wobec profili objętych kontrolą, pomocy w wykrywaniu przez użytkownika wszelkich przypadków niewłaściwego wykorzystania Danych osobowych powiązanych z tymi profilami oraz komunikowaniu się z użytkownikiem i profilami objętymi kontrolą. Prócz tego Symantec będzie wykorzystywać zagregowane, pozbawione elementów identyfikacyjnych, zanonimizowane albo w inny sposób uniemożliwiające identyfikację użytkownika dane pozyskane ze zgromadzonych danych, takich jak dane statystyczne, do następujących celów: • prowadzenie ogólnych badań w obszarze cyberbezpieczeństwa; • zwiększanie wykrywalności złośliwego oprogramowania i zagrożeń dla cyberbezpieczeństwa, np. poprzez analizę próbek plików; • monitorowanie i publikowanie raportów na temat bezpieczeństwa i tendencji oraz zagrożeń związanych z kradzieżą tożsamości;

	przesłać do Symantec w przypadku problemu z Produktami i Usługami i który może obejmować język systemu, ustawienia regionalne kraju, system operacyjny i procesy/pliki uruchomione w momencie wystąpienia błędu 4. Informacje na temat kontroli rodzicielskiej i jej ustawienia, określone i skonfigurowane przez użytkownika, w tym zablokowane witryny, odwiedzane witryny oraz informacje dotyczące filtra czasu i treści, a także adresy URL witryn określonych jako niebezpieczne albo potencjalnie niebezpieczne.	• prowadzenie analiz statystycznych zastosowania produktów, w tym analizy tendencji i porównań w zagregowanych bazach użytkowników; • monitorowanie i podnoszenie wydajności produktów pod względem ich dostępności i szybkości działania; • poznanie częstości komunikacji związanej z produktami w celu optymalizacji ogólnego komfortu użytkownika; oraz • zdobywanie innych informacji biznesowych i rynkowych niezwiązanych z konkretnymi użytkownikami w celu podnoszenia wydajności naszych działań.

Norton Safe Search, Strona główna Norton, Norton Safe Web

Opis Produktu/Usługi	**Dostęp do danych i ich gromadzenie**	**Przetwarzanie danych**
Norton Safe Search to witryna wyszukiwarki internetowej, która umożliwia ochronę użytkownika przed niebezpiecznymi witrynami dzięki filtrowaniu wyników wyszukiwania i wyświetlaniu użytkownikowi ocen bezpieczeństwa poszczególnych witryn, co zapewnia zwiększone bezpieczeństwo podczas aktywności w sieci. To również rozszerzenie przeglądarki, które umożliwia uzyskanie dostępu do witryny internetowej Norton Safe Search na wiele sposobów. Różne wersje tego rozszerzenia mogą w zależności od wyboru użytkownika działać na zasadzie: a) zastąpienia domyślnej wyszukiwarki przeglądarki witryną Norton Safe Search albo b) zastąpienia domyślnej	1. Informacje na temat subskrybenta i dane dotyczące urządzenia oraz oprogramowania, w tym: nazwa, wersja i preferowany język przeglądarki; system operacyjny, wersja albo platforma; adres IP urządzenia użytkownika 2. Dane dotyczące sposobu użycia usługi, w tym: linki w mediach społecznościowych i webmail; przeglądane witryny internetowe; terminy wyszukiwane w Internecie; domyślne treści wprowadzanie w różnych polach wyszukiwania zarządzane przez produkty Norton; wyniki wyszukiwania w wyszukiwarce 3. Pliki cookie, tagi pikselowe, skrypty albo podobne technologie umieszczane na	1. Symantec przetwarza informacje na temat subskrybenta i dane dotyczące urządzenia oraz oprogramowania w celu: • umożliwienia działania Usługi i jej optymalizacji; • zarządzania licencjami; • poznania sposobu i preferencji użycia produktu w celu jego personalizacji i zwiększenia komfortu użytkownika; • przeprowadzania użytkownika przez proces instalacji; • wprowadzania ulepszeń Produktów i Usług, lepszej ochrony użytkownika, jego sieci, urządzenia, danych i tożsamości; oraz • zwiększania zadowolenia klientów ze świadczonych usług za pośrednictwem własnych i zewnętrznych centrów obsługi telefonicznej. 2. Dane dotyczące sposobu użycia usługi są przetwarzane przez Symantec i w imieniu Symantec w celu: • informowania użytkownika o bezpieczeństwie witryn internetowych; • blokowania przeglądania niebezpiecznych witryn; oraz • przeprowadzania analizy sposobu użycia Usługi. Zapytania wyszukiwania wprowadzone przez użytkownika za pośrednictwem naszego produktu Norton Safe Search będą przekierowywane do naszych Zewnętrznych partnerów wyszukiwania Oath/Yahoo! (w przypadku użytkowników ze Stanów Zjednoczonych i Kanady) i IACI (w przypadku użytkowników spoza Stanów Zjednoczonych/Kanady) w celu zwrócenia wyników zapytania użytkownikowi. Nasi Partnerzy zewnętrzni mogą również gromadzić informacje bezpośrednio od Państwa w wyniku Państwa aktywności w Norton Safe Search. Nasi Partnerzy zewnętrzni będą gromadzić takie dane jako administratorzy danych do celów przetworzenia Państwa zapytania wyszukiwania. Gromadzenie danych w powyższy sposób podlega postanowieniom Polityki prywatności, Oświadczenia i Informacji o ochronie prywatności Partnerów zewnętrznych. By umożliwić Państwu korzystanie z Norton Safe Search, złożone przez Państwa zapytania wyszukiwania będą przekierowywane do naszych Partnerów zewnętrznych (tj. niebędących spółkami Symantec), którzy będą przetwarzać Państwa zapytania. Partnerzy zewnętrzni mogą również gromadzić informacje bezpośrednio od Państwa za pośrednictwem Państwa aktywności w Norton Safe Search (łącznie „Dane przekazywane partnerom zewnętrznym"). Partnerzy zewnętrzni będą administratorami danych do celów przetworzenia Państwa zapytania wyszukiwania i z tego powodu to Partnerzy zewnętrzni, a nie Symantec, decydują o sposobie gromadzenia, wykorzystywania, ujawniania, przechowywania Danych przekazywanych partnerom zewnętrznym albo ich przetwarzania w inny sposób. Państwa Dane przekazywane partnerom zewnętrznym podlegają postanowieniom oświadczeń o ochronie prywatności Partnerów

wyszukiwarki przeglądarki witryną Norton Safe Search ORAZ zastąpienia domyślnej strony głównej przeglądarki i nowych kart witryną Strony głównej Norton. Strona główna Norton jest rozszerzeniem przeglądarki i domyślną stroną główną umożliwiającą korzystanie z witryny Norton Safe Search. Norton Safe Web jest rozszerzeniem przeglądarki, które umożliwia użytkownikowi monitorowanie aktywności w sieci i zawartości stron internetowych. Wykorzystuje ono usługi określenia reputacji oraz analizę zawartości strony internetowej w celu ochrony użytkownika przed szkodliwą zawartością witryny internetowej, phishingiem i innymi zagrożeniami.	komputerze albo urządzeniu przez witrynę Norton Safe Search i Stronę główną Norton	zewnętrznych dotyczących przetwarzania Państwa danych w celu zwrócenia wyników zapytania. Prosimy o zapoznanie się z oświadczeniami o ochronie prywatności naszych Partnerów zewnętrznych. 3. Pliki cookie i podobne narzędzia do śledzenia są przetwarzane do celów śledzenia preferencji i historii korzystania z funkcji. Więcej informacji na temat plików cookie można znaleźć w rozdziale zatytułowanym „Technologie śledzenia, pliki cookie i sygnały «nie śledź»" zawartym powyżej w Globalnym oświadczeniu o ochronie prywatności Norton Symantec. Zanonimizowane adresy IP i informacje dotyczące sposobu użycia produktu są przetwarzane w protokole Measurement Protocol Google Analytics w celu przeprowadzania analizy statystycznej błędów krytycznych i zarządzania nimi. Prosimy kliknąć tutaj, aby uzyskać więcej informacji na temat zabezpieczeń danych Google Analytics. Prócz tego Symantec będzie wykorzystywać zagregowane, pozbawione elementów identyfikacyjnych, zanonimizowane albo w inny sposób uniemożliwiające identyfikację użytkownika dane pozyskane ze zgromadzonych danych, takich jak dane statystyczne, do następujących celów: • prowadzenie ogólnych badań w obszarze cyberbezpieczeństwa; • zwiększanie wykrywalności złośliwego oprogramowania i zagrożeń dla cyberbezpieczeństwa, np. poprzez analizę próbek plików; • monitorowanie i publikowanie raportów na temat bezpieczeństwa i tendencji oraz zagrożeń związanych z kradzieżą tożsamości; • prowadzenie analiz statystycznych zastosowania produktów, w tym analizy tendencji i porównań w zagregowanych bazach użytkowników; oraz • monitorowanie i podnoszenie wydajności produktów pod względem ich dostępności i szybkości działania.

Norton Security Toolbar

Opis Produktu/Usługi	Dostęp do danych i ich gromadzenie	Przetwarzanie danych
Norton Security Toolbar występuje w dwóch wariantach: a) jako dodatek do przeglądarki Microsoft Internet Explorer oraz b) jako rozszerzenie przeglądarki Google Chrome. Oba warianty są wykorzystywane przez użytkownika w celu monitorowania aktywności użytkownika w sieci i zawartości stron internetowych. Wykorzystują	1. Dane dotyczące urządzenia oraz oprogramowania, w tym: nazwa, wersja i preferowany język przeglądarki; system operacyjny, wersja albo platforma; adres IP urządzenia użytkownika 2. Dane dotyczące sposobu użycia produktu, w tym: przeglądane witryny internetowe; ograniczona	1. Symantec przetwarza dane dotyczące urządzenia oraz oprogramowania w celu: • umożliwienia działania Usługi i jej optymalizacji; • zarządzania licencjami; • poznania sposobu i preferencji użycia produktu w celu jego personalizacji i zwiększenia komfortu użytkownika; • przeprowadzania użytkownika przez proces instalacji; • wprowadzania ulepszeń Produktów i Usług, lepszej ochrony użytkownika, jego sieci, urządzenia, danych i tożsamości; oraz • zwiększania zadowolenia klientów ze świadczonych usług za pośrednictwem własnych i zewnętrznych centrów obsługi telefonicznej. 2. Dane dotyczące sposobu użycia produktu są przetwarzane przez Symantec i w imieniu Symantec w celu: • informowania użytkownika o bezpieczeństwie witryn internetowych;

one usługi określenia reputacji oraz analizę zawartości strony internetowej w celu ochrony użytkownika przed szkodliwą zawartością witryny internetowej, phishingiem i innymi zagrożeniami. Wariant dla przeglądarki Internet Explorer umożliwia dostęp do informacji w magazynie Norton Identity Safe i korzystanie z nich w interfejsie użytkownika przeglądarki. Zapewnia on również pole wyszukiwania, które umożliwia wyszukiwanie zapytań w witrynie internetowej Norton Safe Search. Wariant dla przeglądarki Google Chrome udostępnia pole wyszukiwania, które umożliwia wyszukiwanie zapytań w witrynie internetowej Norton Safe Search.	historia przeglądania witryn internetowych; terminy wyszukiwane w Internecie; domyślne treści wprowadzanie w różnych polach wyszukiwania zarządzane przez produkty Norton; wyniki wyszukiwania w wyszukiwarce 3. Pliki cookie, tagi pikselowe, skrypty albo podobne technologie umieszczane na komputerze albo urządzeniu przez witrynę Norton Safe Search i Stronę główną Norton	• blokowania przeglądania niebezpiecznych witryn; oraz • przeprowadzania analizy sposobu użycia Usługi. 3. Pliki cookie i podobne narzędzia do śledzenia są przetwarzane do celów śledzenia preferencji i historii korzystania z funkcji. Więcej informacji na temat plików cookie można znaleźć w rozdziale zatytułowanym „Technologie śledzenia, pliki cookie i sygnały «nie śledź»” zawartym powyżej w Globalnym oświadczeniu o ochronie prywatności Norton Symantec. Prócz tego Symantec będzie wykorzystywać zagregowane, pozbawione elementów identyfikacyjnych, zanonimizowane albo w inny sposób uniemożliwiające identyfikację użytkownika dane pozyskane ze zgromadzonych danych, takich jak dane statystyczne, do następujących celów: • prowadzenie ogólnych badań w obszarze cyberbezpieczeństwa; • zwiększanie wykrywalności złośliwego oprogramowania i zagrożeń dla cyberbezpieczeństwa, np. poprzez analizę próbek plików; • monitorowanie i publikowanie raportów na temat bezpieczeństwa i tendencji oraz zagrożeń związanych z kradzieżą tożsamości; • prowadzenie analiz statystycznych zastosowania produktów, w tym analizy tendencji i porównań w zagregowanych bazach użytkowników; oraz • monitorowanie i podnoszenie wydajności produktów pod względem ich dostępności i szybkości działania.

Norton Identity Safe

Opis Produktu/Usługi	Dostęp do danych i ich gromadzenie	Przetwarzanie danych
Norton Identity Safe występuje w dwóch wariantach: a) jako element pakietu Norton Security oraz b) jako rozszerzenie większości przeglądarek, z wyjątkiem przeglądarki Internet Explorer. Wszystkie warianty są menadżerami haseł i umożliwiają zarządzanie nazwami użytkownika, hasłami i innymi przydatnymi informacjami podczas aktywności w sieci.	1. Informacje na temat subskrybenta i dane dotyczące urządzenia oraz oprogramowania, w tym: nazwa, wersja i preferowany język przeglądarki; system operacyjny, wersja albo platforma; adres IP urządzenia użytkownika; *inne Dane osobowe ujawnione przez użytkownika, które mogą obejmować nazwy użytkowników, hasła, adresy witryn internetowych, adresy pocztowe, numery rachunków płatniczych, informacje dotyczące ważności i dowolny tekst 2. Dane dotyczące sposobu użycia usługi, w tym: przeglądane witryny internetowe; terminy wyszukiwane w Internecie; domyślne treści wprowadzanie w różnych polach wyszukiwania zarządzane przez produkty Norton; wyniki wyszukiwania w wyszukiwarce	1. Symantec przetwarza dane dotyczące urządzenia oraz oprogramowania w celu: • umożliwienia działania Usługi i jej optymalizacji; • zarządzania licencjami; • poznania sposobu i preferencji użycia produktu w celu jego personalizacji i zwiększenia komfortu użytkownika; • przeprowadzania użytkownika przez proces instalacji; • wprowadzania ulepszeń Produktów i Usług, lepszej ochrony użytkownika, jego sieci, urządzenia, danych i tożsamości; oraz • zwiększania zadowolenia klientów ze świadczonych usług za pośrednictwem własnych i zewnętrznych centrów obsługi telefonicznej. 2. Dane dotyczące sposobu użycia produktu są przetwarzane przez Symantec i w imieniu Symantec w celu: • informowania użytkownika o bezpieczeństwie witryn internetowych; • blokowania przeglądania niebezpiecznych witryn; oraz • przeprowadzania analizy sposobu użycia Usługi. Zanonimizowane adresy IP i informacje dotyczące sposobu użycia produktu są przetwarzane w protokole Measurement Protocol Google Analytics w celu przeprowadzania analizy statystycznej błędów krytycznych i zarządzania nimi. Prosimy kliknąć tutaj, aby uzyskać więcej informacji na temat zabezpieczeń danych Google Analytics. Prócz tego Symantec będzie wykorzystywać zagregowane, pozbawione elementów identyfikacyjnych, zanonimizowane albo w inny sposób uniemożliwiające identyfikację użytkownika dane pozyskane ze zgromadzonych danych, takich jak dane statystyczne, do następujących celów: • prowadzenie ogólnych badań w obszarze cyberbezpieczeństwa; • zwiększanie wykrywalności złośliwego oprogramowania i zagrożeń dla cyberbezpieczeństwa, np. poprzez analizę próbek plików; • monitorowanie i publikowanie raportów na temat bezpieczeństwa i tendencji oraz zagrożeń związanych z kradzieżą tożsamości; • prowadzenie analiz statystycznych zastosowania produktów, w tym analizy tendencji i porównań w zagregowanych bazach użytkowników; oraz • monitorowanie i podnoszenie wydajności produktów pod względem ich dostępności i szybkości działania.

Norton Family Premier

Opis Produktu/Usługi	Dostęp do danych i ich gromadzenie	Przetwarzanie danych
Norton Family Premier umożliwia ochronę chronionych użytkowników oraz tym urządzeń, które subskrybent zdecyduje się chronić mechanizmami kontroli rodzicielskiej wdrożonymi za pośrednictwem ustawień i funkcji zabezpieczających określonych przez subskrybenta i przez niego zarządzanych. Dodatkowe informacje dotyczące Norton Family Premier znajdują się w rozdziale zatytułowanym „Dodatkowe informacje dotyczące Norton Family Premier” poniżej	*1. Informacje na temat subskrybenta takie jak: dane kontaktowe administratora, w tym w szczególności imię i nazwisko, adres e-mail i hasło subskrybenta zabezpieczające jego konto; Dane osobowe przekazane przez subskrybenta w procesie konfiguracji Usługi albo podczas jakiejkolwiek późniejszej rozmowy z działem obsługi. 2. Dane dotyczące urządzenia oraz oprogramowania, w tym: status instalacji oprogramowania klienckiego Norton Family na urządzeniu subskrybenta albo na urządzeniu chronionego użytkownika; konfiguracja oprogramowania, szczegóły dotyczące produktu i status instalacji; status licencji, informacje dotyczące uprawnień licencyjnych, identyfikator licencji i użytkowanie licencji; nazwa urządzenia, rodzaj, wersja systemu operacyjnego, język, lokalizacja (system nawigacji satelitarnej GPS), rodzaj i wersja przeglądarki; urządzenie, oprogramowanie urządzenia i lista aplikacji; konfiguracje dostępu do aplikacji i baz danych, wymogi wynikające z polityki i status zgodności z polityką, a także dzienniki wyjątków aplikacji i dzienniki błędów w przepływie pracy. *3. Informacje dotyczące chronionego użytkownika, które subskrybent zdecyduje się ujawnić Symantec, w tym: imię i nazwisko, płeć, wiek i rok urodzenia; obrazki awatarów; ostatnie sześć cyfr państwowych numerów identyfikacyjnych powiązanych z chronionym użytkownikiem (np. jeżeli dostępne: numer ubezpieczenia społecznego, krajowy numer identyfikacyjny), adres e-mail, numer telefonu komórkowego, nazwa szkoły i wszystkie inne informacje, które subskrybent chciałby objąć ochroną; szczegółowe informacje dotyczące konta logowania do urządzenia, państwo i strefa czasowa. 4. Informacje dotyczące aktywności w sieci chronionego użytkownika, których monitorowanie subskrybent zlecił Symantec, w tym zależnie od wyboru subskrybenta: aktywność w sieci i na urządzeniach mobilnych oraz lokalizacja; witryny internetowe, do których chroniony użytkownik próbuje uzyskać dostęp, a które Produkt blokuje przed chronionym użytkownikiem; terminy wyszukiwane przez chronionego użytkownika w Internecie; aplikacje, które chroniony użytkownik instaluje albo odinstalowuje na swoim urządzeniu, jeżeli subskrybent aktywował funkcję monitorowania aplikacji; czas korzystania przez chronionego użytkownika z urządzenia; *nazwa profilu chronionego użytkownika, adres URL profilu, wiek, identyfikator profilu Facebook i obejrzane filmy; filmy oglądane przez chronionego użytkownika na YouTube lub Hulu, jeżeli subskrybent aktywował funkcję monitorowania filmów.	1. Symantec przetwarza informacje na temat subskrybenta w celu: • umożliwienia działania Norton Family i jego optymalizacji; • zapewniania wsparcia albo pomocy w usuwaniu błędów; • wysyłania subskrybentowi informacji promocyjnych za zgodą subskrybenta albo zgodnie z przepisami obowiązującego prawa; oraz • założenia Konta Norton subskrybenta. 2. Symantec przetwarza dane dotyczące urządzenia oraz oprogramowania w celu: • zapewniania prawidłowego funkcjonowania Produktu i świadczenia Usług zamówionych przez subskrybenta; • zarządzania licencjami; • oceny i poprawy wskaźnika udanej instalacji Produktu; • na potrzeby badań i rozwoju, których celem jest ulepszanie produktów i usług Symantec i lepsza ochrona sieci subskrybentów i chronionych użytkowników, ich urządzeń, danych i tożsamości. 3. Informacje dotyczące chronionych użytkowników są przetwarzane w celu: • określenia tożsamości i uwierzytelniania subskrybenta i chronionego użytkownika przez Symantec; • udzielania pomocy w wykrywaniu przez subskrybenta wszelkich przypadków niewłaściwego wykorzystania Danych osobowych chronionego użytkownika; oraz • komunikacji z subskrybentem oraz za jego zgodą z chronionym użytkownikiem w celu świadczenia Usługi. 4. Informacje dotyczące aktywności chronionych użytkowników są przetwarzane w celu: • udzielania pomocy w nadzorowaniu przez subskrybenta aktywności w sieci na urządzeniu chronionego użytkownika; • ograniczenia szkód powstałych w wyniku instalacji złośliwego oprogramowania; • udzielania pomocy w egzekwowaniu zasad określonych przez subskrybenta dotyczących aktywności w sieci na urządzeniu chronionego użytkownika; • umożliwienia subskrybentowi wykrycia zagrożeń, na które chroniony użytkownik jest narażony za pośrednictwem komunikacji w sieci albo wiadomości SMS/MMS; oraz • udzielania pomocy subskrybentowi w zabezpieczaniu chronionych użytkowników przed takimi zagrożeniami. Prócz tego Symantec będzie wykorzystywać zagregowane, pozbawione elementów identyfikacyjnych, zanonimizowane albo w inny sposób uniemożliwiające identyfikację użytkownika dane pozyskane ze zgromadzonych danych, takich jak dane statystyczne, do następujących celów: • prowadzenie ogólnych badań w obszarze cyberbezpieczeństwa; • zwiększanie wykrywalności złośliwego oprogramowania i zagrożeń dla cyberbezpieczeństwa, np. poprzez analizę próbek plików; • monitorowanie i publikowanie raportów na temat bezpieczeństwa i tendencji oraz zagrożeń związanych z kradzieżą tożsamości; oraz • prowadzenie analiz statystycznych zastosowania produktów, w tym analizy tendencji i porównań w zagregowanych bazach użytkowników.

Dodatkowe informacje dotyczące Norton Family Premier

Jeżeli subskrybent zdecyduje się aktywować usługę, Norton Family uniemożliwi chronionemu użytkownikowi udostępnianie swoich Danych osobowych.

W zakresie dozwolonym przepisami prawa obowiązującymi w państwie albo regionie będącym miejscem zamieszkania subskrybenta, Symantec może świadczyć usługę **Nadzorowanie wiadomości tekstowych**, która umożliwia subskrybentowi blokowanie albo monitorowanie przychodzących i wychodzących wiadomości tekstowych („SMS") i multimedialnych („MMS") na telefonie komórkowym chronionego użytkownika, a także **usługę Nadzorowanie lokalizacji**. Nadzorowanie wymiany wiadomości SMS i MMS lub lokalizacji, a także korzystanie z wszelkiej dokumentacji takiego nadzoru może być ograniczone albo zabronione na mocy przepisów prawa miejscowego właściwego dla subskrybenta. Przed aktywowaniem tej funkcji subskrybent powinien bezwzględnie zasięgnąć informacji u miejscowych organów.

Po aktywowaniu przez subskrybenta usługi Nadzorowanie lokalizacji Norton Family wypełni polecenie subskrybenta i wykorzysta system GPS w celu śledzenia i ustalenia geolokalizacji urządzenia mobilnego wyznaczonego przez subskrybenta. By umożliwić Norton Family śledzenie, ustalenie, wykorzystanie i ujawnienie geolokalizacji wyznaczonego urządzenia, wymagana jest zgoda subskrybenta i w stosownych przypadkach zgoda użytkownika urządzenia mobilnego albo zgoda osoby sprawującej władzę rodzicielską albo opiekę nad tym użytkownikiem. Odpowiednia zgoda bądź zgody są uzyskiwane za pośrednictwem portalu internetowego Norton albo w stosownych przypadkach w produkcie oraz zostają potwierdzone w momencie wprowadzenia przez subskrybenta informacji dotyczących jego karty płatniczej w celu dokonania zakupu tej Usługi u Symantec przez Internet. Mogą Państwo wycofać każdą udzieloną zgodę w dowolnym momencie. Więcej informacji na temat sposobu wycofania swojej zgody można znaleźć w rozdziale „Prawo do prywatności" Globalnego oświadczenia o ochronie prywatności Norton Symantec. Po zakończeniu świadczenia Usługi informacje dotyczące konta subskrybenta związane z tą Usługą zostaną usunięte.

Po pobraniu przez subskrybenta aplikacji na wyznaczone urządzenie mobilne, Symantec może ustalać geolokalizację tego urządzenia nawet jeżeli aplikacja nie jest używana. Ujawnimy informacje na temat geolokalizacji wyłącznie subskrybentowi, by mógł on zlokalizować urządzenie i będziemy przetwarzać je tylko do celów operacyjnych polegających na świadczeniu usług i funkcji zamówionych przez subskrybenta. Subskrybent nie może wykorzystywać usługi Nadzorowanie lokalizacji Produktu w celu monitorowania danych, lokalizacji, aktywności ani jakichkolwiek innych aspektów związanych z jakąkolwiek osobą, nad którą subskrybent nie sprawuje władzy rodzicielskiej ani opieki. Subskrybenci z Europejskiego Obszaru Gospodarczego powinni porozmawiać z chronionymi użytkownikami pozostającymi pod ich władzą rodzicielską albo opieką, w szczególności jeżeli użytkownicy ukończyli 13 lat, a także powinni podjąć wszelkie niezbędne działania w celu wyjaśnienia chronionym użytkownikom, co oznacza korzystanie przez subskrybenta z Produktu i powiązanych Usług. W przypadku podjęcia decyzji o skorzystaniu z Produktu i powiązanych Usług subskrybent ponosi wyłączną odpowiedzialność za przestrzeganie wszelkich obowiązujących przepisów prawa dotyczących jego relacji z chronionym użytkownikiem i sprawowania władzy rodzicielskiej albo opieki nad nim.

Nadzorowanie wiadomości tekstowych

Usługa Nadzorowanie wiadomości tekstowych jest domyślnie wyłączona. Subskrybent musi osobno włączyć usługę Nadzorowanie wiadomości tekstowych i zainstalować Norton Family na urządzeniu mobilnym, które ma podlegać nadzorowi. Po aktywacji usługa Nadzorowanie wiadomości tekstowych gromadzi następujące informacje z wyznaczonego urządzenia:

- numer telefonu komórkowego urządzenia, które podlega nadzorowi oraz numery telefonów komórkowych innych urządzeń, z którymi zachodzi wymiana wiadomości SMS i MMS;
- treść przychodzących i wychodzących wiadomości SMS na wyznaczonym urządzeniu (w przypadku wymiany wiadomości MMS Symantec nie będzie zapisywać ani pobierać żadnych treści multimedialnych, a jedynie zapisze fakt zaistnienia wymiany wiadomości MMS);
- nazwa kontaktu z książki adresowej powiązana na wyznaczonym urządzeniu z numerem telefonu komórkowego, z którego wysyłane są wiadomości SMS i MMS na wyznaczone urządzenie albo na które takie wiadomości są wysyłane z wyznaczonego urządzenia, jeżeli takie informacje są dostępne;
- znacznik daty/czasu rozmowy;
- lokalizacja wyznaczonego urządzenia;
- dziennik zdarzeń zablokowanych wiadomości SMS/MMS, w tym numery telefonów stron i powiązane nazwy kontaktów, jeżeli są dostępne w książce adresowej na wyznaczonym urządzeniu.

Przed rozpoczęciem nadzoru wychodzących lub przychodzących wiadomości SMS albo MMS na wyznaczonym przez subskrybenta urządzeniu mobilnym Symantec wyśle powiadomienie SMS na wyznaczone urządzenie zawierające informację dla użytkownika urządzenia, że Produkt będzie wypełniać polecenia subskrybenta dotyczące utrwalania i monitorowania treści wiadomości SMS albo MMS, których wymiana odbywa się na wyznaczonym urządzeniu. Jeżeli po otrzymaniu powiadomienia SMS wymiana wiadomości SMS albo MMS nadal będzie się odbywać na wyznaczonym urządzeniu, utrwalanie i monitorowanie wiadomości do celów określonych w niniejszej Informacji rozpocznie się zgodnie z poleceniami subskrybenta. Symantec będzie ponownie wysyłać to samo powiadomienie SMS na wyznaczone urządzenie raz w miesiącu albo każdorazowo przy rozpoczęciu nowej konwersacji.
Jeżeli subskrybent zdecyduje się zablokować wszystkie wiadomości SMS albo MMS albo wymianę wiadomości z określoną osobą, powiadomimy o tym użytkownika wyznaczonego urządzenia i wyślemy wiadomość tekstową do osoby, z którą zachodzi wymiana wiadomości, zawierającą informację, że wymiana wiadomości została zablokowana, a wiadomość nie może zostać dostarczona.