Microsoft

Sekretess

Aktuell information om Microsofts rutiner för databehandling finns i Microsofts sekretesspolicy. Här kan du också läsa om de senaste verktygen vi tillhandahåller för att du ska få tillgång till och kontrollera dina data, och hur du kontaktar oss om du har frågor om sekretess.

Sekretesspolicy för Windows 8 och Windows Server 2012

Senast uppdaterad: **augusti 2012**

I den här snabböversikten över den fullständiga Sekretesspolicy för Windows 8 och Windows Server 2012 sekretesspolicyn (”Windows sekretesspolicy”) beskrivs några av rutinerna för insamling och användning av data i Windows 8 och Windows Server 2012 (”Windows”). Den här informationen fokuserar på funktioner som kommunicerar med Internet och är inte avsedd att vara en fullständig beskrivning. Den gäller inte för andra webbplatser, produkter eller tjänster från Microsoft, varken i online- eller offlineversioner.

Den här sekretesspolicyn innehåller fyra avsnitt:

- Snabböversikt (den här sidan)
- Policyn, det vill säga den fullständiga sekretesspolicyn för Windows som innehåller länkar till Windows-funktioner, som i sin tur har egna policyer
- Funktioner (tillägg), som beskriver de funktioner som påverkar sekretessen i Windows 8 och Windows Server 2012

- Server (tillägg), som beskriver de ytterligare funktioner som påverkar sekretessen i Windows Server 2012

Mer information om hur du kan skydda din dator, din personliga information och din familj på Internet finns på Microsofts säkerhetscenter.

Din information

- Vissa Windows-funktioner kan be om ditt tillstånd att samla in eller använda information från din dator, inklusive personlig information. Windows använder den här informationen på det sätt som anges i den fullständiga Windows sekretesspolicy, i Funktioner (tillägg) och i Server (tillägg).
- Vissa Windows-funktioner kan, med ditt medgivande, dela personlig information via Internet.
- Om du väljer att registrera programvaran blir du ombedd att uppge personlig information.
- Anledningen till att Windows måste aktiveras är att vi vill minska piratkopieringen och säkerställa att våra kunder får den programvarukvalitet de förväntar sig. Vid aktiveringen skickas viss information om din dator till Microsoft.
- Du kan välja att logga in på Windows med ett Microsoft-konto. Det gör att du kan synkronisera Windows-inställningar och logga in automatiskt på appar och webbplatser. När du skapar ett Microsoft-konto blir du ombedd att ange personlig information.
- Ytterligare information

Överst på sidan

Dina alternativ

- I Windows finns flera sätt att ställa in hur informationsöverföringen via Internet ska fungera för Windows-funktioner. Mer information om hur du ställer in dessa funktioner finns i avsnitten Funktioner (tillägg) och

Server (tillägg).

- Vissa funktioner som använder Internet är aktiverade som standard för att göra upplevelsen bättre.
- Ytterligare information

Överst på sidan

Användning av information

- Vi använder den insamlade informationen till att aktivera de funktioner som du använder och tillhandahålla tjänster som du begärt. Vi använder också den också till att förbättra våra produkter och tjänster. För att kunna tillhandahålla våra tjänster uppger vi ibland information till andra företag som arbetar åt oss. Endast företag som behöver informationen i arbetssyfte har åtkomst till den. Dessa företag måste hålla denna information konfidentiell och får inte använda informationen i något annat syfte.
- Ytterligare information

Överst på sidan

Kontakta oss

Mer information om våra sekretessrutiner finns i den fullständiga Windows sekretesspolicy. Du kan också skriva till oss via vårt webbformulär.

Överst på sidan

Microsoft

Sekretess

Aktuell information om Microsofts rutiner för databehandling finns i Microsofts sekretesspolicy. Här kan du också läsa om de senaste verktygen vi tillhandahåller för att du ska få tillgång till och kontrollera dina data, och hur du kontaktar oss om du har frågor om sekretess.

Sekretesspolicy för Windows 8 och Windows Server 2012

På den här sidan

Ytterligare sekretesspolicyer

Det här policyn gäller Windows 8 och Windows Server 2012 (”Windows”). Vissa Windows-komponenter har en egen sekretesspolicy som visas till höger på den här sidan. Sekretesspolicyer för program och tjänster som hör till Windows och sekretesspolicyer för tidigare versioner visas också där.

Information om specifika funktioner finns i Funktioner (tillägg) och Server (tillägg).

Den här policyn fokuserar på funktioner som kommunicerar med Internet och är inte avsedd att vara en fullständig beskrivning.

Insamling och användning av din information

Den personliga information vi samlar in från dig används av Microsoft och företagets dotterbolag och filialer för att aktivera de funktioner du använder och tillhandahålla de tjänster eller utföra de transaktioner som du har begärt eller godkänt. Informationen kan även användas till att analysera och förbättra Microsofts produkter och tjänster.

Förutom vad som beskrivs i denna policy överför vi inte dina

Microsofts felrapporteringstjänst

Microsoft Online

Microsoft Windows-verktyget Borttagning av skadlig programvara

Update Services

Windows Media Center

Windows Media Player

Windows 7

personliga uppgifter till tredje part utan ditt medgivande. Vi anlitar ibland andra företag för att tillhandahålla begränsade tjänster åt oss, till exempel för att utföra statistiska analyser av våra tjänster. Dessa leverantörer har endast tillstånd att inhämta den personliga information som krävs för leverans av tjänsten och de är förbjudna att använda denna information i något annat syfte.

Microsoft kan komma åt eller lämna ut information om dig, inklusive innehållet i dina kommunikationer, i syfte att: (a) efterleva lagen eller uppfylla laglig begäran eller fullgöra rättsliga åtgärder, (b) skydda rättigheter eller egendom som tillhör Microsoft eller Microsofts kunder, inklusive efterlevnaden av Microsofts avtal eller policyer som reglerar användningen av programvaran eller (c) agera för att skydda den personliga säkerheten för Microsofts anställda, Microsofts kunder eller allmänheten.

Information som samlas in av eller skickas till Microsoft av Windows 8 kan lagras och behandlas i USA eller i andra länder där Microsoft eller företagets filialer, dotterbolag eller leverantörer har lokaler. Microsoft följer de riktlinjer som skapats av USA:s handelsdepartement avseende insamling, användning och förvaring av data från EU, EES-området och Schweiz.

Överst på sidan

Insamling och användning av information om din dator

När du använder programvara med Internetaktiverade funktioner skickas information om din dator (”standardinformation om datorn”) till webbplatserna du besöker och onlinetjänsterna du använder. Standardinformationen om datorn innehåller vanligen uppgifter som IP-adress, operativsystemets version, webbläsarens version samt nationella inställningar och språkinställningar. I vissa fall kan den även omfatta maskinvaru-ID, vilket anger enhetens tillverkare, namn och version. När information skickas till Microsoft från en separat funktion eller tjänst skickas även standardinformation om datorn.

Sekretessinformation för varje Windows 8-funktion i Funktioner (tillägg) och Server (tillägg), liksom de funktioner som anges på

den här sidan, beskriver vilken ytterligare information som samlas in och hur den används.

Administratörer kan använda Grupprincip för att ändra flera av inställningarna för de funktioner som beskrivs nedan. Mer information finns i detta white paper för administratörer.

Överst på sidan

Så här skyddas din information

Microsoft arbetar hårt för att skydda din personliga information. Vi använder många olika säkerhetstekniker och -processer för att skydda din information från obehörig åtkomst, användning eller utelämning. Exempelvis lagrar vi den information du tillhandahåller i system med begränsad åtkomst. Dessa system finns i kontrollerade lokaler. Vid överföring av mycket känsliga data (till exempel kreditkortsnummer och lösenord) via Internet, skyddar vi dessa med kryptering, t.ex. SSL-protokollet (Secure Socket Layer).

Överst på sidan

Ändringar i den här sekretesspolicyn

Vi kan komma att uppdatera den här sekretesspolicyn för att återspegla ändringar i våra produkter och tjänster och till följd av feedback från våra kunder. När vi gör det uppdaterar vi datumet vid ”senast uppdaterad” överst i sekretesspolicyn. I samband med ändringar av innehållet i den här sekretesspolicyn eller i hur Microsoft använder din personliga information, meddelar vi dig antingen genom att publicera ett meddelande om ändringen innan den implementeras eller genom att skicka ett meddelande direkt till dig. Vi uppmuntrar dig att regelbundet läsa den här sekretesspolicyn så att du håller dig uppdaterad om hur Microsoft skyddar din personliga information.

Överst på sidan

Mer information

Microsoft tar gärna del av dina kommentarer om denna

sekretesspolicy. Om du har frågor om denna policy, eller anser att vi inte har följt den, kan du kontakta oss via vårt webbformulär.

Microsoft Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052
USA

Överst på sidan

Microsoft

Sekretess

Aktuell information om Microsofts rutiner för databehandling finns i Microsofts sekretesspolicy. Här kan du också läsa om de senaste verktygen vi tillhandahåller för att du ska få tillgång till och kontrollera dina data, och hur du kontaktar oss om du har frågor om sekretess.

Sekretesspolicy för Windows 8 och Windows Server 2012

På den här sidan

Senast uppdaterad: oktober 2012

Observera att den här sidan är ett tillägg till sekretesspolicyn för Windows 8 och Windows Server 2012 ("sekretesspolicyn för Windows"), som innehåller fyra avsnitt:

- I Fokus
- Den fullständiga sekretesspolicyn för Windows som innehåller länkar till sekretesspolicyer för funktioner i Windows som har egna, fristående policyer
- Funktioner (tillägg) – det här dokumentet – som beskriver de funktioner i Windows 8 och Windows Server 2012 som påverkar din integritet
- Server (tillägg), som beskriver de ytterligare funktioner som påverkar integriteten i Windows Server 2012

Om du ska förstå de principer för insamling och användning av data som är relevanta för en särskild funktion eller tjänst

Anpassa handskrift – automatisk inlärning

Hemgrupp

IME (Input Method Editor)

Installationsförbättringsprogram

Internetutskrift

Språkinställningar

Platstjänster

Namn och profilbild

Network Awareness

Aviseringar, appar på låsskärmen och paneluppdateringar

Beställ foton

Assistenten för programkompatibilitet

Egenskaper

Närhet

Fjärråtkomstanslutningar

RemoteApp- och fjärrskrivbordsanslutningar

Anslutning till fjärrskrivbord

Logga in med ett Microsoft-konto

Synkronisera inställningarna

Teredo-teknik

TPM-tjänster (Trusted Platform Module)

Uppdatera rotcertifikat

i Windows bör du läsa den fullständiga sekretesspolicyn och eventuella tillägg eller fristående dokument.

Aktivering

Vad kan jag göra med den här funktionen?

Aktivering minskar problemet med piratkopiering, vilket säkerställer att Microsofts kunder får programvara med den kvalitet de förväntar sig. När programvaran har aktiverats associeras en specifik produktnyckel med den dator (eller maskinvara) som programmet är installerat på. Associationen hindrar att produktnyckeln används för att aktivera samma kopia av programvaran på flera datorer. En del ändringar av datorns komponenter eller programvara kan kräva att du aktiverar programvaran igen. En del ändringar av datorns maskinvara eller programvara kan kräva att du aktiverar Windows igen. Aktiveringsfunktionen kan identifiera och inaktivera kryphål i aktiveringsfunktionen (program som kommer runt eller tar sig förbi aktiveringsfunktionen). Om det finns ett aktiveringskryphål kan en program- eller maskinvaruleverantör ha mixtrat med Microsofts äkta program för att skapa piratkopior av programvaran. Aktiveringskryphål kan störa systemets normala funktion.

Information som samlas in, bearbetas eller överförs

Vid aktiveringen skickas följande uppgifter till Microsoft:

- Microsofts produktkod (en fem siffror lång kod som identifierar den Windows-produkt som du aktiverar).
- Ett kanal-ID eller en platskod som visar hur du erhöll Windows-produkten. Ett kanal-ID eller en platskod kan t.ex. visa om du köpte produkten från en butik, om du fick den som utvärderingsexemplar, om du fick den genom ett volymlicensprogram eller om den installerades i förväg av en datortillverkare.
- Installationsdatumet och huruvida installationen lyckades.

Uppdateringstjänster

Windows Customer Experience Improvement Program (CEIP)

Windows Defender

Windows Felrapportering

Windows Filassociation

Windows Hjälp

Fjärrhjälp

Windows Search

Windows Dela

Windows SmartScreen

Windows Taligenkänning

Windows Store

Tjänsten Windows Time

Windows Felsökning

- Information som underlättar bekräftelsen av att produktnyckeln för Windows inte har ändrats.
- Datormärke och modell.
- Versionsinformation om operativsystemet och programvaran.
- Region- och språkinställningar.
- Ett unikt tal som kallas en GUID (Globally Unique Identifier) som tilldelas datorn.
- Produktnyckeln (i form av ett hashvärde) och produktens ID.
- BIOS-namn, versionsnummer och ändringsdatum.
- Hårddiskvolymens serienummer (i form av ett hashvärde).
- Resultatet av aktiveringskontrollen. Detta innefattar felkoder och följande information om eventuella aktiveringskryphål och relaterad skadlig eller obehörig programvara som har upptäckts eller inaktiverats:
    - Aktiveringskryphålets ID.
    - Aktiveringskryphålets aktuella tillstånd, t.ex. rensad eller försatt i karantän.
    - Datortillverkarens ID.
    - Aktiveringskryphålets filnamn och hashvärde, samt ett hashvärde av relaterade programkomponenter som kan tyda på att datorn är utrustad med ett aktiveringskryphål.
- Namnet och hashvärdet för innehållet i datorns startinstruktionsfil. Om du prenumererar på Windows-licensen skickas även information om hur prenumerationen fungerar. Dessutom skickas standardinformation om datorn, men dess IP-adress

behåller vi bara tillfälligt.

Användning av informationen

Microsoft använder informationen för att bekräfta att du har ett licensierat exemplar av programvaran. Microsoft använder inte informationen för att kontakta enskilda konsumenter.

Val och kontroll

Aktivering är obligatoriskt och sker automatiskt under installationen av Windows. Om du inte har en giltig licens till programvaran kan du inte aktivera Windows.

Överst på sidan

Active Directory Rights Management Services-klienten (AD RMS)

Vad kan jag göra med den här funktionen?

Active Directory Rights Management Services-klienten (AD RMS) är en informationsskyddsteknik som fungerar med program med stöd för AD RMS som skyddar digital information mot obehörig användning. Ägare till digital information kan ange exakt hur mottagare ska få använda informationen i en fil, till exempel vem som kan öppna, ändra, skriva ut eller utföra andra åtgärder med filen. Om du ska kunna skapa eller visa en fil med begränsad behörighet måste din dator köra en app med stöd för AD RMS och ha tillgång till en AD RMS-server.

Information som samlas in, bearbetas eller överförs

AD RMS använder din e-postadress för att identifiera dig hos en AD RMS-server. Därför lagras din e-postadress på servern och på din dator i licenser och identitetscertifikat som servern skapar. Identitetscertifikat och licenser överförs till och från AD RMS-servrar när du försöker öppna, skriva ut eller utföra andra åtgärder på ett dokument som skyddas genom rättighetshantering. Om datorn är ansluten till ett företagsnätverk brukar AD RMS-

servern skötas av företaget. Om du använder Windows Live AD RMS-tjänster sköts servern av Microsoft. För din säkerhet krypteras informationen innan den skickas till Microsoft AD RMS-servrarna.

Användning av informationen

Licensen ger till dig tillgång till skyddade filer. Identitetscertifikaten används för att identifiera dig hos en AD RMS-server och ger dig möjlighet att skydda och komma åt skyddade filer.

Val och kontroll

Funktionerna i AD RMS måste vara aktiverade i en app med stöd för AD RMS. De är inte aktiverade som standard. Du kan välja att inte aktivera eller använda dem. Men om du inte aktiverar dem, kan du inte komma åt skyddade filer.

Överst på sidan

Granskning

Granskning ger en administratör möjlighet att konfigurera Windows att spara information om åtgärder i operativsystemet i en säkerhetslogg som går att granska i Loggboken och andra appar. Med den här loggen kan administratören upptäcka obehörig åtkomst till datorn eller resurser på den. Med den här loggen kan administratörerna till exempel felsöka problem och ta reda på om någon har loggat in på datorn, skapat ett nytt användarkonto, ändrat en säkerhetsprincip eller öppnat ett dokument.

Information som samlas in, bearbetas eller överförs

Administratörer bestämmer vilka uppgifter som samlas in, hur länge de sparas och huruvida de skickas till någon annan. Informationen kan inbegripa personuppgifter, t.ex. användarnamn eller filnamn. Kontakta administratören om du vill ha mer information. Ingen information skickas till Microsoft.

Användning av informationen

Administratörer bestämmer även hur granskningsinformationen används. I allmänhet används säkerhetsloggen av granskare och administratörer för att spåra aktiviteter på datorn eller för att identifiera obehörig åtkomst till datorn eller resurser på den.

Val och kontroll

Administratörer bestämmer om denna funktion är aktiverad eller inte och hur användarna meddelas. Andra användare kan inte se säkerhetsloggen om inte administratören ger dem tillgång till den. Du kan konfigurera granskning på datorn genom att öppna Lokal säkerhetsprincip i Administrationsverktyg.

Överst på sidan

BitLocker-diskkryptering

Vad kan jag göra med den här funktionen?

BitLocker-diskkryptering skyddar dina data genom att kryptera dem, vilket kan hindra en obehörig användare från att komma åt dem. När BitLocker är aktiverat på en enhet som stöds, krypteras informationen på hårddisken av Windows.

Information som samlas in, bearbetas eller överförs

När BitLocker använder programvarukryptering krypteras och dekrypteras data med hjälp av kryptografiska nycklar i minnet samtidigt som de läses från eller skrivs till den skyddade hårddisken. När BitLocker använder maskinvarukryptering utförs krypteringen och dekrypteringen av maskinvaruenheten.

Under konfigurationen av BitLocker kan du välja om du vill skriva ut en återställningsnyckel eller spara den på en plats i nätverket. Om du konfigurerar BitLocker på en fast hårddisk kan du även spara återställningsnyckeln på ett USB-minne.

Om datorn inte tillhör en domän kan du säkerhetskopiera

BitLocker-återställningsnyckeln, återställningsnyckelns ID och datorns namn till OneDrive. Information skickas krypterad via SSL för att skydda din integritet.

Du kan ställa in BitLocker så att data krypteras med ett certifikat som lagras på ett smartkort. När du skyddar en dataenhet med ett smartkort, lagras smartkortets offentliga nyckel och unika identifierare okrypterade på enheten. Den här informationen kan användas för att hitta det certifikat som användes för att generera smartkortets krypteringscertifikat.

Om datorn har säkerhetsmaskinvara med minst version 1.2 av Trusted Platform Module (TPM), använder BitLocker TPM för att på maskinvaruväg skydda data på den disk där Windows är installerat. Mer information finns i avsnittet om Trusted Platform Module (TPM) Services. På datorer med TPM kan du även skapa en PIN-kod och på så sätt skydda krypterade data ännu bättre. BitLocker lagrar denna TPM-baserade PIN-kod i hashat och krypterat format på disken.

Informationen som samlas in av BitLocker skickas inte till Microsoft såvida du inte väljer att säkerhetskopiera återställningsnyckeln till OneDrive.

Användning av informationen

Kryptografiska nycklar och GUID (globalt unika identifierar) lagras i datorns minne så att BitLocker kan fungera. Återställningsinformationen för BitLocker gör att du kan få tillgång till de data som skyddas ifall maskinvaran skulle gå sönder eller om du råkar ut för andra problem. Återställningsinformationen gör att BitLocker kan skilja mellan behöriga och obehöriga användare.

Microsoft använder inte dina enskilda återställningsnycklar för något ändamål. När återställningsnycklar skickas till OneDrive kan Microsoft använda samlade uppgifter om dem för att analysera trender och förbättra sina produkter och tjänster.

Val och kontroll

BitLocker är inaktiverat som standard. På en flyttbar enhet kan alla användare aktivera eller inaktivera BitLocker när som helst genom att öppna BitLocker-diskkryptering på Kontrollpanelen. Administratörer kan aktivera eller inaktivera BitLocker på alla diskar.

Om du har valt att säkerhetskopiera återställningsnycklarna till OneDrive, kan du komma åt eller ta bort nyckeln här.

Överst på sidan

Enhetsidentifiering och konfiguration

Windows innehåller flera funktioner som hjälper dig att identifiera och ställa in enheter på datorn, däribland enheter, mobila bredbandsenheter, nätverksidentifiering och koppling av trådlösa enheter.

Enhetsinstallation

Vad kan jag göra med den här funktionen?

När en ny enhet installeras på datorn kan Windows automatiskt söka efter, ladda ned och installera enhetens drivrutin. Windows kan även ladda ned information om enheten, t.ex. dess beskrivning, bild och tillverkarens logotyp. Vissa enheter, däribland vissa skrivare, webbkameror, mobila bredbandsenheter och bärbara enheter som synkroniserar med Windows, har en app som ger bättre tillgång till enhetens funktioner och gör den lättare att använda. Om tillverkaren av enheten har tagit fram en app till enheten kan Windows ladda ned och installera den automatiskt från Windows Store om du har loggat in där.

Information som samlas in, bearbetas eller överförs

När Windows söker efter drivrutiner kontrollerar operativsystemet först om det redan finns en lämplig drivrutin på datorn. Om det inte finns någon kontaktas Windows Update-tjänsten online för att söka efter och ladda ned enhetsdrivrutiner. Om du vill veta mer om informationen som samlas in av Windows Update och hur

den används kan du läsa sekretesspolicyn för uppdateringstjänsterna.

För att hämta information om enheten och se om det finns en app för den, skickar Windows data om enheten till Microsoft, däribland dess ID (t.ex. dess maskinvaru-ID eller modell-ID), din region och ditt språk samt datumet då enhetsinformationen senast uppdaterades. Om det finns information eller en enhetsapp laddas den ned av Windows från Windows Store och installeras. Appen blir tillgänglig i ditt Windows Store-konto i listan över appar som du har laddat ned.

Användning av informationen

Informationen som skickas till Microsoft används för att leta reda på och ladda ned den lämpliga enhetsdrivrutinen, informationen och appen för enheten. Microsoft använder inte informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Om du väljer snabbinställningarna när du konfigurerar Windows aktiveras automatiskt nedladdning och installation av enhetsdrivrutiner, information och appar. Om du väljer anpassade inställningar kan du bestämma om enhetsdrivrutiner, appar och information ska laddas ned och installeras automatiskt genom att välja **Hämta drivrutiner, appar och information för nya enheter automatiskt** under Skydda och uppdatera datorn. När du har konfigurerat Windows kan du ändra dessa inställningar på Kontrollpanelen genom att välja Ändra installationsinställningarna för enheten och därefter **Nej, jag väljer själv vad som ska göras**.

Du kan när som helst avinstallera en enhetsapp utan att avinstallera enheten, även om du kan behöva appen för att använda vissa av enhetens funktioner. Du kan installera om en enhetsapp efter att ha avinstallerat den genom att använda listan över appar som du äger i Windows Store.

Installation av en mobil bredbandsenhet

Vad kan jag göra med den här funktionen?

Om datorn är utrustad med maskinvara för mobilt bredband från vissa mobiloperatörer kan Windows automatiskt ladda ned och installera en app som gör att du kan hantera kontot och datatrafiken hos den mobiloperatör som stod för datorns mobila bredbandsmaskinvara. Ytterligare information om enheten laddas också ned för att visa den mobila bredbandsanslutningen i nätverkslistan.

Information som samlas in, bearbetas eller överförs

För att det ska gå att ta reda på vilken enhetsinformation och app som ska laddas ned skickar, Windows en del av maskinvarans ID från den mobila bredbandsmaskinvaran. Det gör att vi kan identifiera mobiloperatören. För att skydda dig skickar Windows inte det fullständiga ID:t för den mobila bredbandsmaskinvaran till Microsoft.

Om mobiloperatören har gett Microsoft tillgång till en app laddar Windows ned och installerar den från Windows Store. När du startar en app efter att den har installerats har den tillgång till den mobila bredbandsmaskinvaran, däribland de unika maskinvaru-ID:n som mobiloperatören kan använda för att identifiera ditt konto.

Användning av informationen

Microsoft använder den del av den mobila bredbandsmaskinvarans ID som Windows skickar för att bedöma vilken operatörs app som ska installeras på datorn. När appen har installerats kan den använda det mobila bredbandets maskinvaru-ID:n. En mobiloperatör skulle t.ex. kunna använda dessa ID:n för att hämta information om kontot och dataplanen på nätet. Hur appen använder denna information bestäms av mobiloperatörens sekretesspolicy.

Val och kontroll

Om du väljer snabbinställningarna när du konfigurerar Windows för första gången, letar Windows efter och

installerar mobiloperatörers appar automatiskt. Du kan aktivera eller inaktivera denna funktion på Kontrollpanelen. Mer information finns i avsnittet Enhetsinstallation ovan.

Du kan när som helst avinstallera en mobiloperatörs app utan att avinstallera den mobila bredbandsmaskinvaran.

Nätverksidentifiering

Vad kan jag göra med den här funktionen?

När du ansluter datorn till ett litet privat nätverk som det du kanske har hemma, kan Windows identifiera andra datorer och delade enheter i nätverket automatiskt och göra din dator synlig för andra i nätverket. Om det finns delade enheter kan Windows ansluta till och installera dem automatiskt. Exempel på delade enheter är skrivare och utökningsenheter för medier, men inte personliga enheter som kameror och mobiltelefoner.

Information som samlas in, bearbetas eller överförs

När du aktiverar delning och anslutning till enheter kan information om datorn, t.ex. dess namn och nätverksadress, sändas ut i det lokala nätverket så att andra datorer kan identifiera och ansluta till den.

För att det ska gå att avgöra om enheter som är anslutna till nätverket bör installeras automatiskt, samlas viss information om nätverket in och skickas till Microsoft. Informationen gäller antalet enheter i nätverket, nätverkstypen (t.ex. ett privat nätverk) samt nätverksenheternas typer och modellnamn. Ingen personlig information samlas in, t.ex. nätverksnamnet eller lösenordet.

Beroende på inställningarna för enhetsinstallation kan Windows skicka viss information skickas till Microsoft och installera enhetsprogramvara på datorn. Mer information finns i avsnittet Installera enhet.

Användning av informationen

Informationen om nätverket som skickas till Microsoft

används för att avgöra vilka enheter i nätverket som bör installeras automatiskt. Microsoft använder inte informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Om du väljer att aktivera delning och ansluta till enheter när du ansluter till ett nätverk, aktiveras nätverksidentifiering för det nätverket. Du kan ändra den här inställningen för det aktuella nätverket genom att klicka på nätverkstypen som anges under nätverkets namn i Nätverks- och delningscenter.

Du kan välja om du vill aktivera nätverksidentifiering över huvud taget och om du vill aktivera automatisk konfiguration av nätverksanslutna enheter genom att välja **Ändra avancerade delningsinställningar** i Nätverks- och delningscenter.

Koppling av trådlösa enheter

Vad kan jag göra med den här funktionen?

I Windows kan du koppla datorn till trådlösa enheter som använder Bluetooth eller Wi-Fi Direct. Wi-Fi Direct är en trådlös teknik som gör det möjligt för enheter att kommunicera direkt med varandra utan att behöva ansluta till ett Wi-Fi-nätverk.

Information som samlas in, bearbetas eller överförs

Om du markerar **Tillåt att Bluetooth-enheter hittar denna dator**i Bluetooth-inställningar sänder Windows ut datorns namn via Bluetooth så att Bluetooth-enheter kan identifiera datorn.

Om du markerar **Lägg till en enhet** i Enheter i Datorinställningar sänder Windows ut datorns namn via Wi-Fi så att Wi-Fi Direct-enheter kan identifiera datorn. När du stänger **Lägg till en enhet**slutar Windows skicka datorns namn via Wi-Fi.

Beroende på inställningarna för enhetsinstallation kan

Windows skicka viss information till Microsoft och installera enhetsprogramvara på datorn när datorn kopplas till trådlösa enheter. Mer information finns i avsnittet Enhetsinstallation ovan.

Användning av informationen

Windows sänder datorns namn så att andra enheter kan identifiera och ansluta till datorn. Datornamnet skickas inte till Microsoft.

Val och kontroll

Om du vill välja huruvida Windows ska skicka ut datorns namn via Bluetooth kan du trycka och hålla ned eller högerklicka på datorn i Enheter och skrivare på Kontrollpanelen, välja **Bluetooth-inställningar**och sedan välja **Tillåt att Bluetooth-enheter upptäcker den här datorn**. Om du inte vill att Windows ska sända ut datorns namn via Wi-Fi när du lägger till enheter kan du stänga av Wi-Fi temporärt i Trådlöst i Datorinställningar innan du lägger till en enhet.

Överst på sidan

DirectAccess

Vad kan jag göra med den här funktionen?

Med DirectAccess kan datorn ansluta till nätverket på din arbetsplats mycket smidigt när den är ansluten till Internet, oavsett var du är.

Information som samlas in, bearbetas eller överförs

Varje gång du startar datorn försöker DirectAccess ansluta till nätverket på din arbetsplats, oavsett om du är där eller inte. När du är ansluten laddar datorn ned principerna för arbetsplatsen och du kan då komma åt konfigurerade resurser i nätverket på arbetsplatsen. Administratören kanske använder DirectAccess-anslutningar för att hantera och övervaka din dator på distans, däribland de webbplatser du besöker även om du inte är på jobbet.

DirectAccess skickar ingen information till Microsoft.

Användning av informationen

Företagets policy bestämmer hur informationen som samlas in av administratören på företaget används.

Val och kontroll

DirectAccess måste konfigureras av administratören på arbetsplatsen med Grupprincip. Administratören kan tillåta dig att inaktivera vissa element i DirectAccess temporärt, men det är bara administratören på arbetsplatsen som kan hindra Windows från att försöka ansluta till arbetsplatsen i administrationssyfte. Om du eller administratören på arbetsplatsen tar bort din dator från arbetsplatsens domän, kan DirectAccess inte längre ansluta.

Överst på sidan

Dynamisk uppdatering

Vad kan jag göra med den här funktionen?

Dynamisk uppdatering innebär att Windows kan hämta de senaste uppdateringarna från Windows Update en gång medan Windows installeras. Om Dynamisk uppdatering hittar några uppdateringar laddas de ned och installeras automatiskt, så att din dator är fullständigt uppdaterad första gången du loggar in på eller använder den.

Information som samlas in, bearbetas eller överförs

Dynamisk uppdatering skickar information till Microsoft om datorns maskinvara i syfte att installera kompatibla drivrutiner. Dynamisk uppdatering kan ladda ned följande uppdateringar till din dator:

- **Installationsuppdateringar.** Viktiga programvaruuppdateringar för installationsfiler som säkerställer en lyckad installation.
- **Uppdateringar av medföljande drivrutiner.** Viktiga drivrutinsuppdateringar för den Windows-

version som du installerar.

Användning av informationen

Dynamisk uppdatering skickar information om datorns maskinvara till Microsoft så att lämpliga drivrutiner för ditt system kan identifieras. Om du vill veta mer om hur informationen som samlas in av Dynamisk uppdatering används kan du läsa sekretesspolicyn för uppdateringstjänsterna.

Val och kontroll

När du börjar installera Windows får du en fråga om du vill ansluta till Internet och installera uppdateringar.

Överst på sidan

Hjälpmedelscenter

Vad kan jag göra med den här funktionen?

Med Hjälpmedelscenter kan du aktivera hjälpmedelsalternativ och inställningar som gör det lättare att använda datorn.

Information som samlas in, bearbetas eller överförs

Om du använder den här funktionen ombeds du att välja påståenden som stämmer in på dig.

Dessa påståenden kan vara:

- Det är svårt att se bilder och text.
- Ljusförhållandena gör det svårt att se bilder på skärmen.
- Jag använder inte ett tangentbord.
- Jag är blind.
- Jag är döv.
- Jag har ett talfel.

Informationen sparas i icke läsbart format och lagras lokalt på datorn.

Användning av informationen

Du får ett antal rekommendationer om konfigurationer med ledning av vilka påståenden du valde. Informationen skickas inte till Microsoft och är inte tillgänglig för andra användare än dig och datoradministratörerna.

Val och kontroll

Du kan välja vilka påståenden som du vill markera genom att gå till Hjälpmedel på Kontrollpanelen. Du kan när som helst ändra dina val. Du kan även välja vilka av rekommendationerna som du vill använda på datorn.

Överst på sidan

Loggboken

Vad kan jag göra med den här funktionen?

Datoranvändare, huvudsakligen administratörer, kan se och hantera händelseloggar i Loggboken. Händelseloggar innehåller information om maskinvaru-, program- och säkerhetshändelser på datorn. Du kan även få information från Microsoft om händelser i händelseloggarna genom att klicka på Onlinehjälp för händelseloggen.

Information som samlas in, bearbetas eller överförs

Händelseloggar innehåller information om händelser som har genererats av alla användare och appar på datorn. Som standard kan alla användare se poster i händelseloggen, men administratörer kan välja att begränsa tillgången till händelseloggarna. Du kan komma åt datorns händelseloggar genom att öppna Loggboken. Se Windows Hjälp och support om du vill veta hur du öppnar Loggboken.

Om du hämtar information om en viss händelse med Onlinehjälp för händelseloggen skickas information om händelsen till Microsoft.

Användning av informationen

Om du hämtar information om en händelse med Onlinehjälp för händelseloggen används de data som skickas om händelsen för att leta reda på och ge dig ytterligare information om händelsen. Gäller det en Microsoft-händelse skickas händelseuppgifterna till Microsoft. Microsoft använder inte informationen för att identifiera, kontakta eller skicka reklam till dig. För händelser som hör till andra leverantörers appar skickas informationen till den plats som utgivaren eller tillverkaren har angett. Om du skickar information om händelser till externa utgivare eller tillverkare är bruket av informationen underställt den tredje partens sekretesspolicy.

Val och kontroll

Administratörer kan välja att begränsa tillgången till loggarna i Loggboken. Användare med fullständig åtkomst till loggarna i Händelseloggen kan tömma dem. Såvida du inte tidigare har gått med på att skicka händelseinformation automatiskt när du klickar på Onlinehjälp för händelseloggen ombeds du att bekräfta att den information som visas för dig får skickas via Internet. Ingen händelseinformation skickas via Internet om du inte ger ditt tillstånd till det. Administratörer kan använda Grupprincip för att välja eller ändra webbplatsen dit händelseinformationen skickas.

Överst på sidan

Family Safety

Vad kan jag göra med den här funktionen?

Family Safety hjälper föräldrar att skydda sina barn när de använder en dator. Föräldrar kan bestämma vilka appar, spel och webbplatser som barnen får använda. Föräldrar kan dessutom ange tidsbegränsningar och få regelbundna aktivitetsrapporter per e-post. Föräldrar kan hantera begränsningar och visa aktivitetsrapporter lokalt på datorn

eller via Internet på webbplatsen Microsoft Family Safety.

Information som samlas in, bearbetas eller överförs

Inställningar för och rapporter från Family Safety om vad barnen gör lagras på din dator. Aktivitetsrapporter kan innehålla uppgifter om hur lång tid datorn har använts, hur lång tid som har tillbringats med enskilda appar och spel samt vilka webbplatser som har besökts (även försök att besöka blockerade webbplatser). Datoradministratörer kan ändra inställningar och visa aktivitetsrapporten.

Om onlinehantering har aktiverats för ett barns konto, kan föräldrarna visa barnets aktivitetsrapport och ändras inställningarna på webbplatsen Microsoft Family Safety. En förälder kan låta andra personer titta på aktivitetsrapporter och ändra inställningar genom att lägga till dem som föräldrar på webbplatsen Microsoft Family Safety. Om den förälder som konfigurerar Family Safety är inloggad i Windows med ett Microsoft-konto är onlinehanteringsfunktionen automatiskt aktiverad.

Om Family Safety konfigureras för ett barns konto och onlinehantering är aktiverat, skickas rapporter om vad barnet har för sig automatiskt per e-post till föräldern en gång per vecka.

Användning av informationen

Windows och webbplatsen Microsoft Family Safety använder informationen som samlas in för att tillhandahålla Family Safety-funktionen. Microsoft kan analysera informationen i aktivitetsloggan i avidentifierat skick av datakvalitetsskäl, men vi använder inte uppgifterna för att identifiera, kontakta eller rikta annonser till enskilda användare.

Val och kontroll

Family Safety är inaktiverat som standard. Du kommer åt Family Safety genom att öppna Family Safety på Kontrollpanelen. Det är bara administratörer som kan aktivera Family Safety och enbart användare utan

administratörsbehörighet kan övervakas eller begränsas. Barnen kan se sina inställningar men inte ändra dem. Om Family Safety aktiveras får barnet ett meddelande om att Family Safety övervakar kontot varje gång barnet loggar in i Windows. Om du anger att ett konto tillhör ett barn när det skapas kan du välja att aktivera Family Safety för kontot.

Om administratören som ställer in ett barns konto är inloggad i Windows med ett Microsoft-konto, är onlinehantering automatiskt aktiverat och rapporter om barnets aktivitet skickas en gång i veckan. Föräldrakonton kan läggas till eller tas bort på webbplatsen Microsoft Family Safety. Vem som helst som har lagts till som förälder på webbplatsen kan se barnets aktivitetsrapport och ändra barnets Family Safety-inställningar, även om föräldern inte är administratör på datorn som barnet använder.

Om Family Safety används på rätt sätt ska bara föräldrar vara administratörer på datorn och barnen ska inte tilldelas administratörsbehörighet. Observera att det kan vara olagligt att använda den här funktionen för att övervaka andra användare (t.ex. vuxna).

Överst på sidan

Fax

Vad kan jag göra med den här funktionen?

Med faxfunktionen kan du skapa och spara faxförsättsblad samt skicka och ta emot fax med din dator och ett externt eller inbyggt faxmodem eller en faxserver.

Information som samlas in, bearbetas eller överförs

Informationen som samlas in är de personuppgifter som anges på faxets försättsblad samt de identifierare som finns i branschens standardfaxprotokoll, t.ex. TSID (Transmitting Subscriber ID) och CSID (Call Subscriber ID). Windows använder ”Fax” som värde på varje ID som standard.

Användning av informationen

Informationen som anges i dialogrutan vid avsändning visas på faxets försättsblad. Identifierare som TSID och CSID kan innehålla godtycklig text och brukar användas av den mottagande faxen eller datorn för att identifiera avsändaren. Ingen information skickas till Microsoft.

Val och kontroll

Faxåtkomsten bestäms av dina kontobehörigheter på datorn. Om inte en faxadministratör ändrar åtkomstinställningarna kan alla användare skicka och ta emot fax. Som standard kan alla användare visa dokumenten som de skickar och alla fax som tas emot på datorn. Administratörer kan se alla faxade dokument, skickade som mottagna, och kan ange faxinställningar, däribland vilka som har behörighet att visa eller hantera fax, samt TSID- och CSID-värdena.

Överst på sidan

Anpassa handskrift – automatisk inlärning

Vad kan jag göra med den här funktionen?

Automatisk inlärning är ett verktyg i Anpassa handskrift som är tillgänglig på pekdatorer eller datorer med en Tablet PC-penna. Den här funktionen samlar in data om vilka ord du använder och hur du skriver dem. Detta hjälper programmet för handskriftsigenkänning att känna igen och förbättra tolkningen av din handstil och de ord du använder samt förbättrar även autokorrigerings- och textförslagen för språk utan någon IME (input method editor).

Information som samlas in, bearbetas eller överförs

Informationen som samlas in av funktionen för automatisk inlärning lagras i varje användares användarprofil på datorn. Alla data lagras i ett särskilt format som inte går att läsa med en textvisningsapp (t.ex. Anteckningar eller WordPad) och är bara tillgängliga för andra användare om de är administratörer av datorn.

Information som samlas in omfattar:

- Text från meddelanden som du skriver och kalenderposter som du skapar i e-postappar (t.ex. Office Outlook eller Windows Live E-post), däribland alla meddelanden som du redan har skickat.
- Pennanteckningar som du skriver i Inmatningspanelen.
- Text som tolkats från pennanteckningar som du skriver i Inmatningspanelen eller skriver på tangentbordet på skärmen.
- Alternativa tecken som du väljer för att korrigera tolkad text.

Användning av informationen

Informationen som samlas in används för att förbättra handstilstolkningen genom att skapa en version av tolkningsprogrammet som är anpassad efter din stil och din vokabulär samt för att aktivera autokorrigering och textförslag medan du skriver på tangentbord på skärmen.

Textexemplen används för att skapa en utökad ordlista. Pennanteckningsexemplen används för att förbättra teckenigenkänningen för varje datoranvändare. Ingen information skickas till Microsoft.

Val och kontroll

Automatisk inlärning är aktiverat som standard. Du kan när som helst aktivera eller inaktivera automatisk inlärning genom att öppna Avancerade inställningar i Språk på Kontrollpanelen. Om du inaktiverar automatisk inlärning tas alla data som har samlats in och sparats med automatisk inlärning bort.

Överst på sidan

Hemgrupp

Vad kan jag göra med den här funktionen?

Med Windows kan du enkelt koppla samman datorer i hemnätverket så att du kan dela bilder, musik, filmer, dokument och enheter. Det går även att strömma medier till enheter i hemnätverket, t.ex. utökningsenheter för medier. Dessa datorer och enheter ingår i din hemgrupp. Du kan skydda hemgruppen med ett lösenord och du kan välja vad du vill dela.

Information som samlas in, bearbetas eller överförs

Du kan komma åt dina filer, t.ex. bilder, videor, musik och dokument, från vilken dator som helst i hemgruppen. När du ansluter till en hemgrupp delas kontoinformation (däribland e-postadressen, visningsnamnet och bilden) för alla Microsoft-konton på datorn med andra i hemgruppen så att det ska gå att aktivera delning med dessa användare.

Användning av informationen

Informationen som samlas in gör det möjligt för datorerna i hemgruppen att ta reda på vilka de ska dela innehåll med och hur det ska presenteras. Ingen information skickas till Microsoft.

Val och kontroll

Du kan lägga till eller ta bort datorer från hemgruppen och bestämma vad som ska delas med de övriga medlemmarna i hemgruppen. Du kan skapa en hemgrupp och hantera dess inställningar genom att öppna Hemgrupp i Datorinställningar.

Överst på sidan

IME (Input Method Editor)

Microsofts IME:er (Input Method Editors) används med östasiatiska språk för att omvandla inmatningar på teckenbordet till ideogram. Det här avsnittet handlar om flera olika funktioner, däribland automatisk IME-justering och IME-förutsägelse, felrapporter för IME-omvandlingar

samt registrering av IME-ord.

Automatisk IME-justering och IME-förutsägelse

Vad kan jag göra med den här funktionen?

Beroende på vilken IME du använder, och dina inställningar, kan dess funktioner för automatisk justering och textförslag spara ord eller ordföljder för att förbättra urvalet av de ideogram som visas.

Information som samlas in, bearbetas eller överförs

Funktioner för automatisk justering (inlärning) och textförslag sparar ett ord eller en ordföljd och hur ofta du använder dem. Information för automatisk justering (med undantag av följer av siffror/symboltecken) lagras i filer för varje datoranvändare.

Användning av informationen

Data om automatisk inlärning och textförslag används av IME:n på datorn för att förbättra urvalet av de ideogram som visas när du använder editorn. Om du väljer att skicka dessa data till Microsoft används de för att förbättra IME och relaterade produkter och tjänster.

Val och kontroll

Med undantag för IME:n för förenklad kinesiska (där förutsägelsefunktionen är avstängd som standard) är funktionerna för automatisk inlärning och textförslag på som standard i de IME:er som stöder dem. De data som samlas in skickas inte automatiskt till Microsoft. Du kan välja om du vill samla in eller skicka dessa data eller inte i Språk på Kontrollpanelen.

Rapporter om IME-konverteringsfel

Vad kan jag göra med den här funktionen?

Om det inträffar fel när ideogram visas eller när inmatningar från tangentbordet omvandlas, kan den här funktionen samla in information om felen, vilket kan underlätta för Microsoft att förbättra sina produkter och

tjänster.

Information som samlas in, bearbetas eller överförs

Rapporterna om IME-konverteringsfel innehåller information om IME-konverteringsfel, t.ex. vad du skrev, det första konverterings- eller förutsägelseresultatet, den sträng du valde i stället, information om den IME du använde och information om hur du använde den. Om du råkar använda IME:n för japanska kan du dessutom välja att ta med information om automatisk inlärning i omvandlingsfelrapporterna.

Användning av informationen

Microsoft använder informationen för att förbättra sina program och tjänster. Microsoft använder inte informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Efter att ett visst antal konverteringsfel har lagrats frågar rapportverktyget för felaktiga konverteringar om du vill skicka en konverteringsfelrapport. Du kan även välja att skicka en konverteringsfelrapport när som helst från rapportverktyget för felaktiga konverteringar. Du kan visa informationen i varje rapport innan du väljer att skicka den. Du kan även välja att skicka konverteringsfelrapporterna automatiskt i IME-inställningar.

Registrering av IME-ord

Vad kan jag göra med den här funktionen?

Beroende på vilken IME du använder vill du kanske använda ordregistrering för att rapportera ord som inte stöds (ord som kanske inte konverteras korrekt till ideogram vid inmatningar från tangentbordet).

Information som samlas in, bearbetas eller överförs

Registreringsrapporter kan innehålla den information som du vill lägga till i dialogrutan Lägg till ord om de ord som rapporteras samt versionsnumret för en IME. Dessa

rapporter kan innehålla personlig information, t.ex. om du lägger till personnamn med hjälp av ordregistrering. Du får tillfälle att granska informationen som skickas i rapporterna innan du väljer att skicka dem.

Användning av informationen

Microsoft använder informationen för att förbättra sina program och tjänster. Microsoft använder inte informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Varje gång du skapar en ordregistreringsrapport får du en fråga om du vill skicka den till Microsoft. Du kan visa informationen i rapporten innan du väljer att skicka den.

Överst på sidan

Installationsförbättringsprogram

Vad kan jag göra med den här funktionen?

Genom den här funktionen skickas en rapport till Microsoft med grundläggande information om datorn och hur du installerade Windows 8. Microsoft använder denna information för att förbättra installationen och för att skapa lösningar på vanliga installationsproblem.

Information som samlas in, bearbetas eller överförs

Rapporten innehåller i allmänhet information om hur installationen gick, t.ex. installationsdatumet, hur lång tid det tog för varje installationsfas att slutföras, huruvida installationen var en uppgradering eller en nyinstallation av produkten, versionsuppgifter, operativsystemets språk, medietypen, datorkonfigurationen samt om installationen lyckades eller inte, jämte eventuella felkoder.

Om du väljer att delta i installationsförbättringsprogrammet skickas rapporten till Microsoft när du är ansluten till Internet. Installationsförbättringsprogrammet slumpar fram

ett tal, som kallas en GUID (globalt unik identifierare), som skickas till Microsoft med rapporten. GUID-värdet gör det möjligt för oss att fastställa vilken information som framöver ska skickas från en viss dator. GUID-värdet innehåller ingen personlig information och används inte för att identifiera dig.

Användning av informationen

Microsoft och våra partner använder rapporten för att förbättra våra program och tjänster. Vi använder GUID-värdet för att korrelera informationen med data som samlas in genom Windows Customer Experience Improvement Program (CEIP), ett program som du kan välja att delta in om du använder Windows 8

Val och kontroll

Du kan välja om du vill delta i det här programmet när du installerar Windows 8 genom att välja **Jag vill hjälpa till att göra installationen av Windows bättre** .

Mer information finns i avsnittet Windows CEIP.

Överst på sidan

Internetutskrift

Vad kan jag göra med den här funktionen?

Med Internetutskrift kan du skriva ut via Internet.

Information som samlas in, bearbetas eller överförs

När du skriver ut med den här funktionen måste du först ansluta och autentisera dig för en utskriftsserver på Internet. Informationen som du måste ge till utskriftsservern beror på vilken säkerhetsnivå som utskriftsservern stöder (du kan t.ex. behöva ange ett användarnamn och ett lösenord). När du är ansluten visas en lista över kompatibla skrivare. Om din dator saknar en skrivardrivrutin för den valda skrivaren kan du välja att ladda ned en drivrutin från utskriftsservern. Eftersom utskrifterna inte krypteras kan det vara möjligt för andra att

se innehållet som skickas.

Användning av informationen

Informationen som samlas in gör att du kan skriva ut på fjärrskrivare. Om du väljer att använda en av Microsofts utskriftsservrar använder vi inte informationen som du ger oss för att identifiera, kontakta eller rikta annonser mot dig. Om du skickar information till ett externt företags utskriftsserver bestäms bruket av informationen som samlas in av företagets sekretesspolicy.

Val och kontroll

Du kan aktivera eller inaktivera Internetutskrift genom att öppna Program och funktioner på Kontrollpanelen och sedan välja **Aktivera eller inaktivera Windows-funktioner**.

Överst på sidan

Språkinställningar

Vad den här funktionen åstadkommer

Du kan lägga till de språk du föredrar att använda i språklistan i Windows 8. Appar och webbplatser visas på det första tillgängliga språket i listan.

Information som samlas in, bearbetas eller överförs

När du besöker webbplatser och installerar appar på din dator, skickas listan över föredragna språk till webbplatserna du besöker och är tillgänglig för apparna du använder, så att de kan visa innehåll på de språk du föredrar.

Användning av informationen

Listan över de språk du föredrar används av Microsofts webbplatser och appar för att tillhandahålla innehåll på de språk du föredrar. Microsoft använder inte någon språkinformation för att identifiera eller kontakta dig. Språkinformation som skickas till eller används av externa

webbplatser och appar är underställd den externa webbplatsens eller apputgivarens sekretesspolicy.

Val och kontroll

Din lista över de språk du föredrar är tillgänglig för de appar du installerar och de webbplatser du besöker. Du kan lägga till eller ta bort språk från den här listan i Språkinställningar på Kontrollpanelen. Om det inte finns några språk i listan skickas det språk som du väljer på fliken Format i Nationella inställningar på Kontrollpanelen till de webbplatser du besöker.

Överst på sidan

Platstjänster

På datorer med Windows syftar ”platstjänster” på det program i Windows och den onlinetjänst Microsoft har för att avgöra ungefär var din dator befinner sig. Dessa uppgifter lämnas till appar eller webbplatser som du låter få tillgång till dem. Windows-positioneringsplattformen hämtar uppgifter om platsen från särskild maskinvara, t.ex. en GPS-sensor i datorn, eller genom program som Windows-platsprovider.

Windows-positioneringsplattformen

Vad kan jag göra med den här funktionen?

Om du väljer att aktivera Windows-positioneringsplattformen ber de appar du installerar från Windows Store dig om tillstånd att komma åt datorns plats. Beroende på hur systemet är konfigurerat kan plattformen ta reda på var datorn finns med hjälp av maskinvara, t.ex. en GPS-sensor eller ett program som Windows-platsprovider.

Plattformen förhindrar inte appar från att få åtkomst till datorns plats på andra sätt. Du kan t.ex. installera enheter (t.ex. en GPS-mottagare) som kan skicka platsinformation direkt till en app och helt gå förbi plattformen. Oavsett vilka inställningar Windows-positioneringsplattformen har, kan

tjänster på nätet använda din dators IP-adress för att ta reda på ungefär var den är – vanligtvis i vilken stad.

Information som samlas in, bearbetas eller överförs

Windows-positioneringsplattformen skickar inte i sig någon information från din dator, men enskilda platsprovidrar (t.ex. Windows-platsprovider) kanske skickar information när du använder positionsmedvetna appar. Appar som har behörighet att använda plattformen för att ta reda på var du befinner dig kan även skicka eller lagra den informationen.

Användning av informationen

Om aktiverar Windows-positioneringsplattformen kan behöriga appar ta reda på var du befinner dig och använda informationen för att leverera personanpassat innehåll. Om du använder en extern app eller platsprovider är dess bruk av information om var datorn befinner sig underställt den externa partens sekretesspolicy. Innan du laddar ned en app från Windows Store bör du kunna se huruvida den är platsmedveten i appbeskrivningen.

Val och kontroll

Om du väljer snabbinställningarna under installationen av Windows aktiverar du Windows-positioneringsplattformen. Om du väljer att anpassa inställningar kan du ställa in Windows-positioneringsplattformen genom att välja **Aktivera Windows-positioneringsplattformen så att appar kan fråga användarna var de befinner sig** under **Dela info med appar**. Första gången varje Store-app begär att få reda på var datorn befinner sig får du en fråga från Windows om du vill tillåta det. Du kan bestämma huruvida appar kan fråga efter din plats i Sekretess i Datorinställningar och du kan bestämma huruvida en enskild Store-app kan använda din plats i Behörigheter i appens snabbknapp Inställningar.

Om du använder en skrivbordsapp som utnyttjar Windows-positioneringsplattformen bör den be om tillstånd att

använda din dators plats, och när den gör det visas en ikon i meddelandefältet för att visa att datorns plats har använts. Varje användare kan bestämma sina egna platsinställningar för alla appar i Sekretess i Datorinställningar. Dessutom kan administratörer välja att inaktivera Windows-positioneringsplattformen i Plats på Kontrollpanelen.

Windows-platsprovider

Vad kan jag göra med den här funktionen?

Windows-platsprovidern ansluter till Microsoft-positioneringstjänsten på nätet, som tar reda på ungefär var datorn befinner sig baserat på vilka Wi-Fi-nätverk som finns i närheten av datorn eller datorns IP-adress.

Information som samlas in, bearbetas eller överförs

När en app som du har gett tillstånd att få information om var du befinner dig ber om att få reda på det, ber Windows-positioneringsplattformen alla installerade platsprovider (däribland Windows-platsprovidern) att ta reda på var du befinner dig nu. Windows-platsprovidern undersöker först om det finns en lista över Wi-Fi-åtkomstpunkter från en tidigare begäran från en platsmedveten app. Om det inte redan finns en lista över Wi-Fi-åtkomstpunkter i närheten, eller om listan är inaktuell, skickar providern information om Wi-Fi-åtkomstpunkter i närheten samt GPS-information (om sådana uppgifter finns) till Microsoft-positioneringstjänsten. Tjänsten skickar tillbaka datorns ungefärliga position till Windows-platsprovider, som skickar platsen till Windows-positioneringsplattformen som i sin tur uppger positionen till den app som begärde datorns plats. Windows-platsprovidern kan dessutom uppdatera sin lagrade lista över Wi-Fi-åtkomstpunkter. Windows-platsprovider underhåller listan så att den kan fastställa datorns ungefärliga position utan att ansluta till Internet varje gång. Listan över åtkomstpunkter krypteras när den lagras på disken så att inga appar kan komma åt den direkt.

Informationen som skickas om Wi-Fi-åtkomstpunkter i närheten omfattar BSSID:t (MAC-adressen för Wi-Fi-åtkomstpunkten) och signalstyrkan. GPS-informationen innehåller den observerade latituden, longituden, riktningen, hastigheten och höjden. För att skydda din integritet skickar Windows-platsprovider någon information som kan identifiera din dator unikt, utöver den standardinformation om datorn som skickas i samband med alla anslutningar till Internet. För att skydda Wi-Fi-nätverksägarnas integritet skickar Windows inga SSID:n (Wi-Fi-åtkomstpunkternas namn) eller dolda Wi-Fi-nätverk. I sekretess- och säkerhetssyfte skickas information om Wi-Fi-nätverk krypterat via SSL.

Användning av informationen

Informationen används av Windows-platsprovidern för att ge Windows-positioneringsplattformen ungefärlig information om var din dator befinner sig när en behörig app begär det.

Om du väljer att hjälpa till att förbättra Microsoft-positioneringstjänsten används den information om Wi-Fi och GPS som du skickar till Microsoft för att förbättra Microsofts positioneringstjänster. Det förbättrar de positioneringstjänster som dina appar får tillgång till. Microsoft lagrar inga data som samlas in från den här tjänsten som skulle kunna användas för att identifiera, kontakta, rikta annonser mot dig eller spåra eller skapa en historik över var din dator har varit.

Val och kontroll

Windows-platsprovidern används bara om en behörig app har begärt att få reda på var datorn befinner sig. Mer information om hur du kan bestämma huruvida appar kan begära att få reda på var datorn befinner sig finns i avsnittet Windows-positioneringsplattformen. Om du ger appar behörighet att fråga var datorn befinner sig tas den cachelagrade listan över närliggande Wi-Fi-åtkomstpunkter som krypteras och lagras av Windows-platsprovidern bort

och ersätts med jämna mellanrum.

Om du väljer snabbinställningarna när du installerar Windows väljer du att hjälpa till att förbättra Microsoft-positioneringstjänsten. Om du väljer anpassade inställningar kan du bestämma om du vill hjälpa till att förbättra Microsoft-positioneringstjänsten genom att välja **Hjälp till att göra Microsoft tjänster ännu bättre genom att skicka positioneringsinformation när appar med positioneringsfunktioner används** under **Skicka info till Microsoft så att vi kan förbättra Windows och apparna**. Efter installationen av Windows kan du ändra inställningen i Positioneringsinställningar på Kontrollpanelen. Om du väljer att inte hjälpa till att förbättra tjänsten kan du ändå använda Windows-platsprovidern för att ta reda på ungefär var datorn befinner sig.

Du kan aktivera eller inaktivera Windows-platsprovidern genom att öppna **Aktivera eller inaktivera Windows-funktioner** på Kontrollpanelen. Om du inaktiverar Windows-platsprovidern kan du ändå använda andra platsprovider (t.ex. GPS) med Windows-positioneringsplattformen.

Överst på sidan

Namn och profilbild

Vad kan jag göra med den här funktionen?

Appar kan begära ditt namn och din profilbild från Windows för att tillhandahålla personligt innehåll. Ditt namn och din profilbild visas under Ditt konto i Användare i Datorinställningar. Om du loggar in i Windows med ett Microsoft-konto använder Windows namnet och profilbilden som hör till kontot. Om du inte har valt en bild till kontot är profilbilden en standardbild som tillhandahålls av Windows.

Information som samlas in, bearbetas eller överförs

Om du tillåter appar att använda ditt namn och din

profilbild ger Windows dessa uppgifter till alla appar som begär dem. Appar kan lagra eller överföra denna information.

Om du loggar in i Windows med ett domänkonto och väljer att tillåta appar att använda ditt namn och din profilbild, tillåts appar som får använda dina autentiseringsuppgifter i Windows att komma åt vissa andra former av information om domänkontot. Dessa uppgifter består bland annat av användarens huvudnamn (t.ex. johanna@contoso.com) och DNS-domännamn (t.ex. corp.contoso.com\johanna).

Om du loggar in i Windows med ett Microsoft-konto eller in i Windows med ett domänkonto som är kopplat till ett Microsoft-konto, kan Windows synkronisera profilbilden på datorn med profilbilden hos Microsoft automatiskt.

Användning av informationen

Om du använder ett externt företags app bestäms appens bruk av namnet och profilbilden av den tredje partens sekretesspolicy. Om du använder en av Microsofts appar har de en egen sekretesspolicy.

Val och kontroll

Om du väljer snabbinställningarna när du installerar Windows tillåter Windows att apparna får tillgång till namnet och profilbilden. Om du väljer att anpassa inställningar kan du ställa in åtkomsten till ditt namn och din profilbild genom att markera **Låt appar använda mitt namn och min profilbild** under **Dela info med appar**. Efter installationen av Windows kan du ändra inställningen i **Sekretess** i Datorinställningar. Du kan ändra kontobilden i **Anpassa** i Datorinställningar. Du kan även välja att tillåta vissa appar att ändra profilbilden.

Överst på sidan

Network Awareness

Vad kan jag göra med den här funktionen?

Om du prenumererar på nätverksåtkomst (t.ex. med en mobil bredbandsanslutning) ger den här funktionen information om prenumerationen till appar och funktioner i Windows på datorn. Funktioner i Windows och appar kan använda dessa uppgifter för att optimera sitt beteende. Om du exempelvis betalar för den mängd data du laddar ned väntar Windows Update med att ladda ned uppdateringar med lägre prioritet till datorn tills du är ansluten till ett annat slags nätverk. Den här funktionen ger även information om nätverksanslutningen, t.ex. signalstyrkan och huruvida datorn är ansluten till Internet.

Information som samlas in, bearbetas eller överförs

Den här funktionen samlar in information om anslutningar till Internet och i intranätet, t.ex. datorns DNS-suffix (Domain Name Service), nätverksnamnet och gatewayadressen till de nätverk som datorn ansluter till. Den här funktionen erhåller även information om abonnemang, t.ex. hur stora datamängder som återstår.

Nätverksanslutningsprofiler kan innehålla en historik över alla besökta nätverk samt datumet och tiden för den senaste anslutningen. Den här funktionen kan försöka kontakta en av Microsofts servrar för att ta reda på om du är ansluten till Internet. De enda data som skickas till Microsoft när nätverksanslutningen kontrolleras är normal datorinformation.

Användning av informationen

Om några data skickas till Microsoft används de bara för att kontrollera nätverksanslutningens status. Nätverksanslutningens status görs tillgänglig för appar och funktioner på datorn som begär information om nätverksanslutningen. Om du använder ett externt företags app bestäms bruket av informationen som samlas in av den tredje partens sekretesspolicy.

Val och kontroll

Network Awareness är aktiverat som standard. En

administratör kan inaktivera funktionen genom att använda alternativet Tjänster i Administrationsverktyg på Kontrollpanelen. Vi rekommenderar inte att du inaktiverar den här funktionen, eftersom vissa funktioner i Windows då inte fungerar som det är tänkt.

Överst på sidan

Aviseringar, appar på låsskärmen och paneluppdateringar

Windows Store-appar kan ta emot innehåll och visa aviseringar automatiskt på flera olika sätt. De kan exempelvis ta emot meddelanden som visas helt kort i hörnet av skärmen eller på appaneler om de är fästa på Start. Du kan även få dessa aviseringar på låsskärmen om du vill det. Låsskärmen kan dessutom visa upp vissa appars detaljerade eller avkortade status. Apputgivare kan skicka innehåll till dina Windows Store-appar genom tjänsten Windows Push Notification Service, som körs på Microsofts servrar, eller så kan apparna ladda ned information direkt från externa servrar.

Aviseringar

Vad kan jag göra med den här funktionen?

Windows Store-appar kan leverera information i realtid eller periodvis. Dessa meddelanden visas en kort stund i hörnet av skärmen.

Information som samlas in, bearbetas eller överförs

Appar kan visa text och/eller bilder i aviseringar. Innehållet i aviseringarna kan tillhandahållas lokalt av appen (t.ex. en klockapp som du har ställt in ett larm i). Aviseringar kan även skickas från en apps onlinetjänst via Windows Push Notification Service (t.ex. en uppdatering från ett socialt nätverk). Bilder som visas i aviseringar kan laddas ned direkt från en server som anges av appens utgivare. I sådana fall skickas normal datorinformation till servern.

Användning av informationen

Microsoft använder bara aviseringsinformation för att leverera aviseringar från dina appar till dig. Aviseringen kan lagras temporärt av Windows Push Notification Service innan den levereras till datorn. Om en avisering inte kan levereras direkt, lagras den bara i ett par minuter innan den tas bort.

Val och kontroll

Du kan inaktivera aviseringar för alla eller enskilda appar i **Aviseringar** i Datorinställningar. Om du inaktiverar aviseringar för en app eller avinstallerar den, kan apputgivaren fortfarande skicka uppdateringar till Windows Push Notification Service, men de visas inte på din dator.

Appar på låsskärmen

Vad kan jag göra med den här funktionen?

Vissa appar kan visa sin status och aviseringar på skärmen när datorn är låst. Appar på låsskärmen kan även utföra aktiviteter i bakgrunden medan du inte använder dem, t.ex. synkronisera e-post.

Information som samlas in, bearbetas eller överförs

Appar på låsskärmen kan ta emot statusuppdateringar från apputgivaren via Windows Push Notification Service eller direkt från apputgivarens (eller någon annans) servrar. Appar på låsskärmen skulle även kunna skicka eller behandla annan information som inte har med aviseringar och uppdateringar att göra.

Användning av informationen

Windows använder status- och meddelandeinformationen från låsskärmsapparna för att uppdatera låsskärmen.

Val och kontroll

När du har installerat Windows ställs apparna E-post, Kalender och Meddelanden in automatiskt som låsskärmsappar. Du kan lägga till eller ta bort dessa eller andra appar från låsskärmen i Anpassa i Datorinställningar. Du kan även välja en app som ständigt visar sin detaljerade

status (t.ex. detaljer om nästa möte i kalendern) på låsskärmen.

Du kan bestämma huruvida appar på låsskärmen får visa aviseringar på låsskärmen i Aviseringar i Datorinställningar.

Paneluppdateringar

Vad kan jag göra med den här funktionen?

Windows Store-appar kan leverera information i realtid eller periodvis till dig. De visas som uppdateringar av apparnas paneler på Startskärmen.

Information som samlas in, bearbetas eller överförs

Store-appar som är fästa på Start kan uppdatera sina paneler med text och/eller bilder. Innehållet som visas på appens panel kan tillhandahållas lokalt av appen, laddas ned med jämna mellanrum från en server som apputgivaren anger eller skickas från en apps nättjänst via Windows Push Notification Service. Om panelinnehållet laddas ned direkt från en server som anges av appens utgivare skickas normal datorinformation till servern.

Användning av informationen

Microsoft använder bara panelinformation för att leverera paneluppdateringar från dina appar till dig. Den här informationen kan lagras temporärt av Windows Push Notification Service innan den levereras till datorn. Om paneluppdateringen inte kan överföras direkt, lagras den bara i ett par dagar innan den tas bort.

Val och kontroll

När en app har börjat ta emot paneluppdateringar, kan du stänga av dem genom att välja appens panel på Start och välja **Stäng av levande panel** bland kommandona som är tillgängliga för appen. Om du plockar bort en apps panel från Start visas inte dess paneluppdateringar. Om du avinstallerar en app kan apputgivaren fortfarande skicka uppdateringar till Windows Push Notification Service, men de visas inte på din dator.

Om du vill ta bort de uppdateringar som visas på panelerna på Start sveper du från höger sida av startskärmen eller pekar i det övre högra hörnet av Start eller klickar på **Inställningar**och trycker eller klickar sedan på **Paneler**. Tryck eller klicka på **Rensa** under **Rensa personlig information i mina paneler**. Paneluppdateringar som levereras efter att du har rensat de aktuella uppdateringarna fortsätter att dyka upp.

Överst på sidan

Beställ foton

Vad kan jag göra med den här funktionen?

Med Beställ foton kan du skicka digitala bilder som lagras på datorn eller en nätverksenhet till en utskriftstjänst på nätet som du väljer själv. Beroende på tjänsten kan du kanske skriva ut dina bilder och få dem levererade per post eller hämta bilderna i någon butik.

Information som samlas in, bearbetas eller överförs

Om du vill beställa framkallning av bilderna skickas de digitala bilderna via Internet till den tjänst som du har valt. Filsökvägen till de digitala bilder som du väljer (som kan innehålla ditt användarnamn) kan skickas till tjänsten så att den kan visa och ladda upp bilderna. Digitala bildfiler kan innehålla data om bilden som lagrades i filen av kameran, t.ex. datumet och tiden då bilden togs, eller platsen där den togs om kameran är utrustad med en GPS. Filerna kan även innehålla personlig information (t.ex. bildtexter) som kan ha kopplats till filen med hjälp av en app för hantering av digitala bilder och Windows Utforskaren. Mer information finns i avsnittet Egenskaper nedan.

När du har valt en framkallningstjänst i Beställ foton tas du till tjänstens webbplats i fönstret Beställ foton. Information som du anger på framkallningstjänstens webbplats överförs till tjänsten.

Användning av informationen

Informationen som lagras i de digitala bildfilerna av kameran kan användas av framkallningstjänsten vid framställningen av bilderna, t.ex. för att justera bildens färger eller skärpa innan den skrivs ut. Information som lagras av program för digital bildhantering kan användas av framkallningstjänsten för att skriva ut bildtexten på fram- eller baksidan av fotot. Framkallningstjänsternas bruk av dessa uppgifter och annan information som du tillhandahåller, t.ex. uppgifter som du anger på webbplatsen, är underställt företagets sekretesspolicy.

Val och kontroll

Du kan använda Beställ foton för att välja vilka foton du vill skicka och vilken framkallningstjänst du vill anlita. Vissa bildbehandlingsprogram kan hjälpa dig med att ta bort lagrad personlig information innan bilderna skickas för utskrift. Du kan kanske även redigera filens egenskaper och ta bort lagrad personlig information.

Överst på sidan

Assistenten för programkompatibilitet

Vad kan jag göra med den här funktionen?

Om det uppstår ett kompatibilitetsproblem med en app du försöker köra försöker Assistenten för programkompatibilitet att hjälpa dig lösa det.

Information som samlas in, bearbetas eller överförs

Om ett problem med kompatibiliteten upptäcks för en app som du försöker köra skapas en rapport med information om appens namn, version, de nödvändiga kompatibilitetsinställningarna och vad du har gjort med appen hittills. Problem med inkompatibla appar rapporteras till Microsoft via Windows Felrapportering eller Windows Customer Experience Improvement Program (CEIP).

Användning av informationen

Felrapporterna används för att ge svar om problem som du

rapporterar om dina appar. Svaren innehåller länkar (om några sådana är tillgängliga) till apputgivarens webbplats så att du kan läsa mer om möjliga lösningar. Felrapporter som skapas när appar kraschar används för att försöka ta reda på vilken inställning som behöver ändras när du stöter på kompatibilitetsproblem med de appar som du kör i den här versionen av Windows. Informationen som rapporteras via programmet för felrapportering i Windows används för att identifiera kompatibilitetsproblem med appar.

Microsoft använder inte någon information som samlas in av den här funktionen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

För problem som rapporteras via Windows Felrapportering skapas en felrapport bara om du väljer alternativet att leta på nätet efter en lösning. Om du inte tidigare har gått med på att rapportera problem automatiskt så att du kan se om det finns någon lösning, får du en fråga om du vill skicka felrapporten. Mer information finns i avsnittet Windows Felrapportering.

Vissa problem rapporteras automatiskt via Windows CEIP om du har valt att aktivera detta. Mer information finns i avsnittet Windows Customer Experience Improvement Program.

Överst på sidan

Egenskaper

Vad kan jag göra med den här funktionen?

Egenskaper är filinformation som du kan använda för att snabbt söka efter och ordna dina filer. Vissa egenskaper hör till själva filen (t.ex. dess storlek) medan andra kan vara specifika för en app eller en enhet (t.ex. kamerainställningarna när du tog ett foto eller platsinformationen som sparades av kameran med fotot).

Information som samlas in, bearbetas eller överförs

Vilken typ av information som lagras beror på filens typ och apparna som använder den. Exempel på egenskaper är filnamnet, ändringsdatumet, filstorleken, författaren, sökord och kommentarer. Egenskaperna lagras i filen och flyttas med den om den flyttas eller kopieras till en annan plats, t.ex. en filresurs, eller om den skickas som en e-postbilaga.

Användning av informationen

Egenskaper kan hjälpa dig att söka efter och ordna dina filer snabbare. De kan även användas av appar för att utföra appspecifika uppgifter. Ingen information skickas till Microsoft.

Val och kontroll

Du kan redigera eller ta bort vissa egenskaper för en fil genom att markera den i Windows Utforskaren och klicka på Egenskaper. Vissa filspecifika egenskaper, t.ex. ändringsdatumet, filstorleken, filnamnet och vissa appspecifika egenskaper, går inte att ta bort på det här viset. Appspecifika egenskaper går bara att ändra eller ta bort om appen som genererade filen stöder dessa funktioner.

Överst på sidan

Närhet

Närhetstjänster

Vad kan jag göra med den här funktionen?

Om din dator är utrustad med NFC-maskinvara (near-field communication) kan du knacka den mot en annan enhet med NFC-maskinvara för att dela länkar, filer och annan information. Det finns två olika typer av närhetsanslutningar: Knackat och klart samt Knacka och håll. Med knacka och gör kan du skapa en kort- eller långvarig anslutning mellan enheter via Wi-Fi, Wi-Fi Direct eller Bluetooth. Med knacka och håll är anslutningen bara

aktiv under den tid som enheterna befinner sig nära varandra.

Information som samlas in, bearbetas eller överförs

När du knackar två enheter med närhetsstöd mot varandra, utbyter de information för att upprätta en anslutning mellan sig. Beroende på hur enheterna är konfigurerade kan dessa data omfatta Bluetooth- och Wi-Fi-nätverksadresser samt datorns namn.

När en anslutning har upprättats kan annan information utbytas mellan enheterna, beroende på den specifika närhetsfunktionen eller appen som du använder. Windows kan skicka filer, länkar och annan information mellan enheter via en närhetsanslutning. Appar som använder närhetsfunktionen kan skicka och ta emot all information de har tillgång till. Informationen kan skickas via din nätverks- eller Internetanslutning eller direkt via en trådlös anslutning mellan enheterna.

Användning av informationen

Nätverks- och datorinformation som byts ut via en närhetsanslutning används för att upprätta en nätverksanslutning samt för att identifiera enheterna som ansluter till varandra. Data som överförs via en närhetsanslutning som har upprättats i en app kan användas på valfritt sätt av den appen. Ingen information skickas till Microsoft.

Val och kontroll

Närhetstjänsten är aktiverad som standard. En administratör kan inaktivera funktionen genom att använda alternativen i Enheter och skrivare på Kontrollpanelen.

Knacka och skicka

Vad kan jag göra med den här funktionen?

Med Knacka och skicka och Windows är det enkelt att dela vald information med en vän som står intill dig eller med någon annan av dina enheter, t.ex. en mobiltelefon. Om du

exempelvis har öppnat en webbläsare kan du starta Knacka och skicka från rutan Enheter. Nästa enhet som du knackar på får en länk till webbsidan som visas. Detta fungerar även med alla appar som stöder informationsdelning, t.ex. bilder, text eller filer.

Information som samlas in, bearbetas eller överförs

Knacka och skicka använder den information som du delar och den information som beskrivs i avsnittet Närhetstjänster ovan.

Användning av informationen

Informationen används bara för att upprätta anslutningen mellan de två enheterna. Den delade informationen lagras inte av Knacka och skicka. Ingen information skickas till Microsoft.

Val och kontroll

Om närhetstjänsten är aktiverad är även Knacka och skicka det. Mer information finns i avsnittet om närhetstjänsten.

Överst på sidan

Fjärråtkomstanslutningar

Vad kan jag göra med den här funktionen?

Med fjärråtkomstanslutningar kan du ansluta till privata nätverk via en VPN-anslutning (virtuellt privat nätverk) och Fjärråtkomsttjänsten (RAS). RAS är en komponent som ansluter en datorklient (vanligtvis din dator) till en värddator (som även kallas fjärråtkomstservern) med hjälp av standardprotokoll i branschen. VPN-tekniker ger användare möjlighet att ansluta till ett privat nätverk, t.ex. ett företagsnätverk, via Internet.

Med fjärråtkomstkomponenten Fjärranslutning kan du ansluta till Internet med ett modem eller en bredbandsteknik såsom ett kabelmodem eller en DSL-anslutning (digital subscriber line). Fjärranslutning innehåller uppringningskomponenter såsom RAS-klient,

Anslutningshanteraren och RAS-telefon, samt uppringningsprogram som används i kommandotolken, t.ex. rasdial.

Information som samlas in, bearbetas eller överförs

Uppringningskomponenterna samlar in information från datorn, t.ex. ditt användarnamn, ditt lösenord och ditt domännamn. Informationen skickas till systemet som du försöker ansluta till. För att skydda dig och din dator krypteras säkerhetsrelaterad information såsom ditt användarnamn och ditt lösenord och lagras på din dator.

Användning av informationen

Uppringningsinformation används för att ansluta din dator till Internet. En fjärråtkomstserver skulle kunna behålla användarnamnet och information om IP-adressen i redovisnings- och regelefterlevnadssyfte, men ingen information skickas till Microsoft.

Val och kontroll

I uppringningskomponenter som inte används i kommandotolken kan du spara ditt lösenord genom att välja **Spara det här användarnamnet och lösenordet**. Du kan när som helst avmarkera alternativet och därmed ta bort det sparade lösenordet från uppringningsprogrammet. Eftersom det här alternativet är inaktiverat som standard kan du uppmanas ange ditt lösenord för att ansluta till Internet eller till ett nätverk. I uppringningsprogram som anropas i kommandotolken, t.ex. rasdial, finns det ingen möjlighet att spara lösenordet.

Överst på sidan

RemoteApp- och fjärrskrivbordsanslutningar

Vad kan jag göra med den här funktionen?

Med RemoteApp- och fjärrskrivbordsanslutningar kan du komma åt appar och skrivbord på fjärrdatorer som har gjorts tillgängliga för fjärråtkomst från nätet.

Information som samlas in, bearbetas eller överförs

När du aktiverar en anslutning laddas konfigurationsfiler ned till din dator från den URL som du anger. Dessa konfigurationsfiler länkar till appar och skrivbord på fjärrdatorerna så att du kan köra dem på din dator. Datorn kontrollerar automatiskt om det har kommit uppdateringar till dessa konfigurationsfiler och laddar ned dem med regelbundna mellanrum. Apparna körs på fjärrdatorerna, och informationen som du anger i apparna överförs via nätverket till fjärrdatorerna som du har valt att ansluta till.

Användning av informationen

Uppdateringar av konfigurationsfiler skulle kunna innehålla inställningsändringar, däribland att du får tillgång till nya appar. De nya apparna körs dock bara om du väljer det. Den här funktionen skickar även information till fjärrdatorerna där fjärrapparna körs. Bruket av dessa data av fjärrapparna är underställt appleverantörernas och fjärrdatoradministratörernas sekretesspolicy. Ingen information skickas till Microsoft.

Val och kontroll

Du kan välja om du vill använda RemoteApp- och fjärrskrivbordsanslutningar eller inte. Du kan lägga till eller ta bort RemoteApp- och fjärrskrivbordsanslutningar genom att öppna RemoteApp- och fjärrskrivbordsanslutningar på Kontrollpanelen. Du kan lägga till en ny anslutning genom att klicka på **Konfigurera en ny anslutning med RemoteApp- och fjärrskrivbordsanslutningar**och ange en anslutnings-URL i dialogrutan. Du kan även ange din e-postadress för att ladda ned anslutnings-URL:en. Du kan ta bort en anslutning och dess anslutningsfiler genom att klicka på **Ta bort** i dialogrutan med anslutningsbeskrivningar. Om du kopplar ifrån en anslutning utan att stänga alla öppna appar förblir de öppna på fjärrdatorn. RemoteApp- och fjärrskrivbordsanslutningar visas inte i listan Lägg till eller ta bort program på Kontrollpanelen.

Överst på sidan

Anslutning till fjärrskrivbord

Vad kan jag göra med den här funktionen?

Anslutning till fjärrskrivbord är ett sätt för dig att upprätta en fjärranslutning till en värddator som kör Fjärrskrivbordstjänster.

Information som samlas in, bearbetas eller överförs

Inställningarna för Anslutning till fjärrskrivbord sparas i det applokala lagringsutrymmet eller i en RDP-fil (Remote Desktop Protocol) på din dator. Dessa inställningar omfattar namnet på din domän och konfigurationsinställningar för anslutningen, t.ex. fjärrdatorns namn, användarnamnet, visningsinformation, lokal enhetsinformation, ljudinformation, urklipp, anslutningsinställningar, namn på fjärrappar och en sessionsikon eller miniatyrbild.

Autentiseringsuppgifter för dessa anslutningar, autentiseringsuppgifter till Fjärrskrivbordsgateway och en lista över betrodda fjärrskrivbordsgatewayservrar lagras lokalt på datorn. Listan lagras permanent om den inte tas bort av en administratör. Ingen information skickas till Microsoft.

Användning av informationen

Med informationen som samlas in av Anslutning till fjärrskrivbord kan du ansluta till värddatorer som kör Fjärrskrivbordstjänster med de inställningar du föredrar. Information om ditt användarnamn, ditt lösenord och din domän samlas in så att du kan spara anslutningsinställningarna och dubbelklicka på RDP-filen eller klicka på en favorit för att öppna en anslutning utan att behöva ange uppgifterna igen.

Val och kontroll

Du kan välja om du vill använda Anslutning till fjärrskrivbord. Om du gör det innehåller RDP-filerna och

Anslutning till fjärrskrivbord-favoriterna den information som krävs för att ansluta till en fjärrdator, däribland de alternativ och inställningar som konfigurerades när anslutningen sparades automatiskt. Du kan ändra RDP-filerna och favoriterna. Det gäller även filer för att ansluta till samma dator med olika inställningar. Om du vill ändra de sparade inloggningsuppgifterna öppnar du Autentiseringshanteraren i Användarkonton på Kontrollpanelen.

Överst på sidan

Logga in med ett Microsoft-konto

Vad kan jag göra med den här funktionen?

Ett Microsoft-konto (som tidigare kallades ett Windows Live ID) är en e-postadress och ett lösenord som du kan använda som inloggningsuppgifter i appar, på webbplatser och i tjänster från Microsoft och utvalda partner till Microsoft. Du kan skaffa dig ett Microsoft-konto i Windows eller på Microsofts webbplatser där du måste logga in med ett Microsoft-konto.

Du kan välja att logga in i Windows med ett Microsoft-konto eller att ansluta ditt lokala konto eller domänkonto till ett Windows-konto. Om du gör det kan Windows hjälpa till så att dina datorer ser likadana ut genom att automatiskt synkronisera inställningar och information i Windows och Microsofts appar. Om du besöker dessa webbplatsers inloggningssidor blir du även automatiskt inloggad på de webbplatser som använder Microsoft-konton för inloggning.

Information som samlas in, bearbetas eller överförs

När du anger en e-postadress som du vill använda som Microsoft-konto då du installerar datorn eller i Användare i Datorinställningar, skickar Windows e-postadressen till Microsoft för att undersöka om det redan finns ett Microsoft-konto som är kopplat till den e-postadressen. Om du redan använder den e-postadressen som Microsoft-

konto, kan du använda den och lösenordet för Microsoft-kontot för att logga in i Windows. Om du inte redan har tillräckligt mycket säkerhetsinformation om ditt Microsoft-konto, kanske vi först ber dig att ange ytterligare säkerhetsinformation, t.ex. ett mobiltelefonnummer, så att vi kan verifiera att kontot är ditt om du har problem med att logga in i kontot. Om du inte har något Microsoft-konto kan du skapa ett med vilken e-postadress som helst.

Varje gång du loggar in i Windows med ett Microsoft-konto medan datorn är ansluten till Internet, verifierar Windows e-postadressen och lösenordet hos Microsofts servrar. När du är inloggad i Windows med ditt Microsoft-konto eller med ett domänkonto som är kopplat till ditt Microsoft-konto:

- Vissa inställningar i Windows synkroniseras mellan datorerna som du loggar in på med ett Microsoft-konto. Mer information om vilka inställningar som synkroniseras och hur du kontrollerar dem finns i avsnittet Synkronisera inställningarna.

- Microsoft-appar som använder ett Microsoft-konto för autentisering (t.ex. E-post, Kalender, Foton, Kontakter, Meddelanden, OneDrive, Microsoft Office och andra appar) kan börja ladda ned din information automatiskt (appen E-post laddar exempelvis automatiskt ned meddelanden som skickas till din Outlook.com- eller Hotmail.com-adress om du har en sådan).

- Webbläsare kan logga in dig automatiskt på webbplatser som du loggar in på med ditt Microsoft-konto (om du t.ex. går till OneDrive.com kan du loggas in automatiskt utan att behöva ange lösenordet för ditt Microsoft-konto igen).

Windows ber dig om tillstånd innan några andra företags appar får använda profilinformationen eller någon annan personlig information som är kopplad till ditt Microsoft-konto. Om du loggar in i Windows med ett domänkonto

som är kopplat till ett Microsoft-konto synkroniseras de inställningar och de uppgifter som du väljer med domänkontot, och du loggas in automatiskt i appar och på webbplatser enligt beskrivningen ovan. Eftersom domänadministratörer kan komma åt all information på din dator, kan de även komma åt alla inställningar och uppgifter som du har valt att synkronisera med andra datorer via ditt Microsoft-konto. Det kan gälla inställningar som ditt namn, din profilbild och din webbläsarhistorik. Mer information om vilka inställningar som synkroniseras och hur du kontrollerar dem finns i avsnittet Synkronisera inställningarna.

Användning av informationen

När du skapar ett nytt Microsoft-konto i Windows använder vi informationen som du anger för att skapa och skydda kontot. Säkerhetsinformationen som du anger (t.ex. telefonnummer och alternativ e-postadress) används endast om du inte kan logga in på ditt konto. När du är inloggad i Windows med ett Microsoft-konto använder Windows Microsoft-kontouppgifterna för att logga in dig i appar och på webbplatser automatiskt. Om du vill veta mer om hur din integritet påverkas av att du har ett Microsoft-konto kan du läsa sekretesspolicyn som visas när du väljer Registrera dig för en ny e-postadress. Mer information om hur enskilda appar från Microsoft använder information som är kopplad till ditt Microsoft-konto finns i dessa appars sekretesspolicy. Du hittar sekretesspolicyn för en app från Microsoft på snabbknappen Inställningar eller i dialogrutan Om.

Val och kontroll

När du loggar in i Windows med ett Microsoft-konto synkroniseras vissa inställningar automatiskt. Information om hur du ändrar vilka Windows-inställningar som synkroniseras eller hur du slutar synkronisera finns i avsnittet Synkronisera inställningar. Mer information om vilka data som samlas in av Microsoft-appar som använder ett Microsoft-konto för autentisering finns i sekretesspolicyn

för respektive app. Du hittar sekretesspolicyer för Windows Live-appar (E-post, Kalender, Foton, Kontakter, Meddelanden, OneDrive) på go.microsoft.com/fwlink/?LinkId=257483och för Microsoft Office på go.microsoft.com/fwlink/?LinkId=257484. Du kan också hitta en apps sekretesspolicy i appens snabbknapp Inställningar eller i dialogruta Om.

Du behöver inte logga in i Windows med ett Microsoft-konto. När du lägger till en datoranvändare i samband med att du konfigurerar datorn eller i **Användare** i Datorinställningar kan du välja att använda ett lokalt konto eller ett Microsoft-konto. Du kan när som helst växla till ett lokalt konto eller ett Microsoft-konto i **Användare** i Datorinställningar. Om du loggar in i Windows med ett domänkonto kan du ansluta eller koppla bort Microsoft-kontot när som helst i **Användare** i Datorinställningar.

När du använder InPrivate-surfning i Internet Explorer loggas du inte in automatiskt på webbplatser som använder Microsoft-konton.

Överst på sidan

Synkronisera inställningarna

Vad kan jag göra med den här funktionen?

När du loggar in i Windows med ett Microsoft-konto synkroniserar Windows vissa av dina inställningar och uppgifter med Microsofts servrar så att det ska bli enklare för dig att anpassa utseendet på flera olika datorer. När du har loggat in på en dator med ett Microsoft-konto och loggar in på en annan dator med samma Microsoft-konto för första gången, laddar Windows ned och tillämpar de inställningar som du har valt att synkronisera från de andra datorerna. De inställningar som du väljer att synkronisera uppdateras automatiskt på Microsofts servrar och dina andra datorer då du använder dem.

Information som samlas in, bearbetas eller överförs

Om du väljer att logga in i Windows med ett Microsoft-konto synkroniserar Windows vissa inställningar med Microsofts servrar. Dessa inställningar omfattar:

- Språkinställningar
- Inställningar för Hjälpmedelscenter
- Anpassade inställningar såsom din profilbild, låsskärmsbild, bakgrund och musinställningar
- Inställningar för Windows Store-appar
- Ordlistor för stavningskontroll och IME
- Webbläsarens historik och favoriter
- Sparade lösenord till appar, webbplatser och nätverk

Alla inställningar som överförs krypteras med SSL för att skydda din integritet. Vissa av dessa inställningar synkroniseras inte på din dator förrän du har lagt till den som en betrodd dator i Microsoft-kontot.

Om du loggar in i Windows med ett domänkonto som är kopplat till ett Microsoft-konto synkroniseras de inställningar och de uppgifter du har valt till domänkontot. Lösenord som du sparar medan du är inloggad i Windows med ett domänkonto som är kopplat till ditt Microsoft-konto synkroniseras aldrig. Eftersom domänadministratörer kan komma åt all information på din dator, kan de även komma åt alla inställningar och uppgifter, däribland webbläsarhistoriken, som du har valt att synkronisera med andra datorer via ditt Microsoft-konto.

Användning av informationen

I Windows 8 används dessa inställningar och uppgifter för att tillhandahålla synkroniseringstjänsten. Microsoft använder inte de synkroniserade inställningarna och uppgifterna för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

När du loggar in i Windows med ett Microsoft-konto synkroniseras inställningarna. Du kan välja om du vill synkronisera inställningarna och vad som synkroniseras genom att gå till **Synkronisera inställningarna** i Datorinställningar. Om du loggar in i Windows med ett domänkonto och du väljer att koppla det till ett Microsoft-konto får du en fråga vilka inställningar du vill synkronisera innan anslutningen till Microsoft-kontot sker.

Överst på sidan

Teredo-teknik

Vad kan jag göra med den här funktionen?

Teredo-teknik (Teredo) innebär att datorer och nätverk kan kommunicera via flera nätverksprotokoll.

Information som samlas in, bearbetas eller överförs

Varje gång du startar datorn, försöker Teredo hitta en öppen IPv6-tjänst (Internet Protocol version 6) på Internet. Detta sker automatiskt när datorn är ansluten till ett offentligt eller privat nätverk, men det sker inte i hanterade nätverk såsom företagsdomäner. Om du använder en app som kräver Teredo för att kunna använda IPv6-anslutningar, eller om du ställer in brandväggen så att IPv6-anslutningar alltid ska vara tillåtna, kontaktar Teredo regelbundet tjänsten Microsoft Teredo via Internet. Den enda information som skickas till Microsoft är normal datorinformation och namnet på den tjänst som efterfrågas (t.ex. teredo.ipv6.microsoft.com).

Användning av informationen

Informationen som skickas från din dator av Teredo används för att ta reda på om datorn är ansluten till Internet och om den kan hitta en öppen IPv6-tjänst. När tjänsten har hittats skickas information för att upprätthålla en anslutning till IPv6-tjänsten.

Val och kontroll

Genom att använda kommandotolkverktyget netsh kan du ändra den fråga som tjänsten skickar via Internet och använda servrar från andra företag än Microsoft i stället, eller så kan du stänga av den. Detaljerade anvisningar finns i avsnittet Internet Protocol Version 6, Teredo och relaterade tekniker i den här tekniska rapporten.

Överst på sidan

TPM-tjänster (Trusted Platform Module)

Vad kan jag göra med den här funktionen?

TPM (Trusted Platform Module) är säkerhetsmaskinvara som ingår i vissa datorer och som om den finns och har allokerats ger datorn möjlighet att utnyttja avancerade säkerhetsfunktioner fullt ut. De funktioner i Windows som utnyttjar TPM är bland andra BitLocker-diskkryptering, Virtuellt smartkort, Säker start, Windows Defender och TPM-baserad certifikatlagring.

Information som samlas in, bearbetas eller överförs

Som standard blir Windows ägare till TPM och lagrar den fullständiga auktoriseringsinformationen om TPM-ägaren, så att den bara är tillgänglig för administratörer av Windows. Begränsade auktoriseringsvärden skapas för att utföra vanliga administrativa åtgärder och åtgärder av standardanvändare och hanteras av Windows.

Med TPM-hanteringskonsolen kan du allokera TPM interaktivt och spara auktoriseringsvärdet för TPM-ägaren på externa medier såsom ett USB-flashminne efter att TPM har allokerats. En sparad fil innehåller auktoriseringsinformationen om TPM-ägaren för TPM. Filen innehåller även datornamnet, operativsystemversionen, information om den skapande användaren och skapelsedatumet så att du känner igen filen.

I domänmiljö kan det fullständiga TPM-ägarlösenordet konfigureras av domänadministratören så att det lagras i Active Directory under ett TPM-objekt när TPM allokeras.

Varje TPM har en unik kryptografisk bekräftelsenyckel som den använder för att visa att den är äkta. Bekräftelsenyckeln kan skapas och lagras i TPM av datortillverkaren, men på gamla datorer kan Windows behöva se till att den skapas i TPM. Den privata delen av bekräftelsenyckeln är i säkert förvar i TPM, och när den har skapas brukar den inte gå att återställa. Ett bekräftelsenyckelcertifikat lagras i TPM på de flesta datorer med Windows 8. Bekräftelsenyckelcertifikatet visar att bekräftelsenyckeln finns i en maskinvaru-TPM. Certifikatet används av fjärrverifierare för att bekräfta att en TPM följer TPM-specifikationerna. Bekräftelsenyckelcertifikatet brukar signeras av TPM-tillverkaren eller plattformtillverkaren.

Användning av informationen

När TPM har initierats kan appar använda den för att skapa och skydda ytterligare unika kryptografiska nycklar. Exempel: BitLocker-diskkryptering utnyttjar TPM för att skydda nyckeln som hårddisken krypteras med.

Om du väljer att spara TPM-ägarens lösenord i en fil ger informationen om datorn och användaren som sparas i filen dig möjlighet att identifiera motsvarande dator och TPM. TPM-bekräftelsenyckeln används av Windows när TPM initieras för att kryptera TPM-ägarens auktoriseringsvärde innan den skickas till TPM. Windows skickar inte kryptografiska nycklar utanför datorn. Windows har ett gränssnitt för andra appar, t.ex. program mot skadlig kod, så att de kan använda bekräftelsenyckeln för vissa TPM-scenarier, t.ex. uppmätt start med attestering. För program som skyddar mot skadlig kod är bekräftelsenyckeln och dess certifikat användbara för att bekräfta startmätningar och tillhandahålls av en TPM från en viss tillverkare. Som standard är det bara administratörer och appar med administrativ behörighet som kan använda TPM-bekräftelsenyckeln.

Val och kontroll

Användare eller administratörer måste aktivt välja att

använda TPM genom att aktivera en funktion i Windows eller köra en app som använder TPM.

Du kan välja att rensa TPM och återställa den till fabriksinställningarna. När TPM rensas tas ägarinformationen bort, och med undantag av bekräftelsenyckeln samtliga TPM-baserade nycklar eller kryptografisk information som appar kan ha skapat när TPM användes.

Överst på sidan

Uppdatera rotcertifikat

Vad kan jag göra med den här funktionen?

Certifikat används huvudsakligen för att verifiera en persons eller enhets identitet, för att autentisera en tjänst eller för att kryptera filer. Betrodda rotcertifikatutfärdare är de organisationer som utfärdar certifikat. Uppdatera rotcertifikat kontaktar tjänsten Windows Update för att se om Microsoft har lagt till en certifikatutfärdare i listan över betrodda utfärdare, men bara om en app tar emot ett certifikat som har utfärdats av en certifikatutfärdare som inte är direkt betrodd (ett certifikat som inte lagras i listan över betrodda certifikat på datorn). Om certifikatutfärdaren har lagts till i Microsofts lista över betrodda utfärdare, läggs dess certifikat automatiskt till i listan över betrodda certifikat på datorn.

Information som samlas in, bearbetas eller överförs

Uppdatera rotcertifikat skickar en begäran till tjänsten Windows Update och frågar efter den aktuella listan över rotcertifikatutfärdare i Microsofts rotcertifikatprogram. Om det icke betrodda certifikatet finns med i listan hämtar Uppdatera rotcertifikat det från Windows Update och sparar det i databasen med betrodda certifikat på datorn. Informationen som överförs är bland annat rotcertifikatens namn och kryptografiska hashvärden.

Mer information om Windows Update och din integritet

finns i sekretesspolicyn för uppdateringstjänsterna.

Användning av informationen

Microsoft använder informationen för att uppdatera listan över betrodda certifikat på din dator. Microsoft använder inte informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Uppdatera rotcertifikat är aktiverat som standard. Administratörer kan konfigurera Grupprincip för att inaktivera Uppdatera rotcertifikat på en dator.

Överst på sidan

Uppdateringstjänster

Vad kan jag göra med den här funktionen?

Uppdateringstjänsterna för Windows omfattar Windows Update och Microsoft Update:

- **Windows Update** är en tjänst där du kan få uppdateringar av Windows-program och andra stödprogram, t.ex. drivrutiner som enhetstillverkare står för.
- **Microsoft Update** är en tjänst där du kan få uppdateringar av Windows-program och andra program från Microsoft, t.ex. Microsoft Office.

Information som samlas in, bearbetas eller överförs

Om du väljer att hämta viktiga programvaruuppdateringar för datorn kan verktyget Borttagning av skadlig programvara (MSRT) medfölja dessa uppdateringar. Verktyget Borttagning av skadlig programvara genomsöker datorn efter ofta förekommande skadlig programvara (malware) och gör det lättare att ta bort identifierade hot som kan smitta datorn. Om verktyget körs tar det bort skadliga program som finns publicerade på webbplatsen Microsoft Support. Under en genomsökning efter skadliga

program skickas en rapport till Microsoft med specifik information om de skadliga program och fel som upptäcks samt annan information om din dator. Mer information finns i sekretesspolicyn för verktyget Borttagning av skadlig programvara i Windows .

Om du vill veta mer om vilken övrig information uppdateringstjänsterna samlar in kan du läsa sekretesspolicyn för uppdateringstjänsterna.

Användning av informationen

Informationen om skadliga program hjälper oss att förbättra våra produkter mot skadliga program och andra säkerhetsprodukter och tjänster. Ingen information i rapporterna om skadliga program används för att identifiera eller kontakta dig.

Om du vill veta mer om hur uppdateringstjänsterna använder information kan du läsa sekretesspolicyn för uppdateringstjänsterna.

Val och kontroll

Om du väljer standardinställningarna när du installerar Windows aktiveras uppdateringstjänsterna och Windows Update konfigureras att installera uppdateringar automatiskt. Om du väljer att anpassa inställningarna kan du hantera uppdateringstjänsterna i **Windows Update** under **Skydda och uppdatera datorn**. När du har installerat Windows kan du ändra inställningarna för uppdateringstjänsterna på Kontrollpanelen. Mer information finns i uppdateringstjänsternas sekretesspolicy.

Om du har valt att söka efter och installera viktiga uppdateringar och Borttagning av skadliga program medföljer uppdateringarna, kan du inaktivera programmets funktion genom att följa dessa anvisningar på Microsoft Support.

Överst på sidan

Windows Customer Experience Improvement Program (CEIP)

Vad kan jag göra med den här funktionen?

Windows Customer Experience Improvement Programs (CEIP) kan samla in information om hur du använder dina appar, dina datorer, dina anslutna enheter och Windows. Dessutom samlar det in information om prestanda- och tillförlitlighetsproblem som kan uppträda. Om du väljer att delta i Windows CEIP skickar Windows dessa data till Microsoft och laddar dessutom regelbundet ned en fil för att samla in mer relevant information om hur du använder Windows och appar. CEIP-rapporter skickas till Microsoft och vi använder dem för att förbättra de funktioner som våra kunder oftast använder för att skapa lösningar på vanliga problem.

Information som samlas in, bearbetas eller överförs

CEIP-rapporter kan även innehålla information som:

- Konfigurationsinformation. däribland information om hur många processorer datorn är utrustad med, antalet nätverksanslutningar som används, bildskärmars upplösning och vilken version av Windows som körs.

- Prestanda- och tillförlitlighetsinformation, däribland information om hur snabbt appar svarar när du klickar på en knapp, hur många problem du upplever med en app eller en enhet samt hur snabbt information skickas eller tas emot via en nätverksanslutning.

- Appbruksinformation, däribland information om de funktioner du använder mest, t.ex. hur ofta du startar appar, hur ofta du använder Windows Hjälp och support, vilka tjänster du använder för att logga in i appar och hur många mappar du brukar skapa på skrivbordet.

CEIP-rapporter innehåller också information om händelser (händelseloggdata) på din dator högst sju dagar innan du

bestämde dig för att delta i CEIP. Eftersom de flesta användare väljer att delta i CEIP inom ett par dagar efter att ha installerat Windows använder Microsoft dessa uppgifter för att analysera och förbättra installationen av Windows.

Informationen skickas till Microsoft när du är ansluten till Internet. CEIP-rapporter innehåller inte avsiktligt någon kontaktinformation, t.ex. ditt namn, din adress eller ditt telefonnummer, men en del rapporter kan oavsiktligt innehålla enskilda identifierare, t.ex. ett serienummer för en enhet som är ansluten till din dator. Microsoft filtrerar informationen i CEIP-rapporterna och försöker ta bort allt i dem som gör att en individ går att identifiera.

CEIP skapar slumpmässigt ett tal som kallas en GUID (globalt unik identifierare) som skickas till Microsoft med varje CEIP-rapport. GUID-värdet gör det möjligt för oss att fastställa vilken information som framöver ska skickas från en viss dator. De förinstallerade apparna från Microsoft som licensieras för bruk med Windows kan skapa egna unika identifierare för bruk med CEIP. De kan baseras på uppgifter från ditt Microsoft-konto.

CEIP laddar dessutom regelbundet ned en fil för att samla in mer relevant information om hur du använder Windows och appar. Den här filen hjälper Windows att samla in ytterligare information för att hjälpa Microsoft att lösa vanliga program och bättre förstå hur Windows och appar används.

Användning av informationen

Microsoft använder CEIP-information för att förbättra sina produkter och tjänster liksom andra företags program och maskinvara som har designats för att användas med dessa produkter och tjänster. Vi kan även dela med oss av CEIP-information till Microsofts partner så att de kan förbättra sina produkter och tjänster, men informationen delas i avidentifierat skick och går inte att använda för att identifiera dig, kontakta dig eller rikta reklam till dig.

Vi använder GUID-värdet för att fastställa hur omfattande den feedback vi får är och hur den ska prioriteras. Med detta GUID kan Microsoft till exempel skilja mellan en kund som får samma problem hundra gånger och hundra kunder som får samma problem en gång. Microsoft använder inte informationen som samlas in av CEIP för att identifiera eller kontakta dig.

Val och kontroll

Om du väljer snabbinställningarna när du konfigurerar Windows aktiveras Windows CEIP: Windows och Microsofts appar som licensieras med Windows kan skicka CEIP-rapporter om alla datorns användare. Om du väljer anpassade inställningar kan du ställa in CEIP genom att välja **Delta i Customer Experience Improvement Program och hjälp till att förbättra Microsofts programvara och tjänster** under **Skicka info till Microsoft så att vi kan förbättra Windows och apparna**. Efter installationen av Windows kan administratörer ändra denna inställning i Åtgärdscenter på Kontrollpanelen.

Mer information finns online i vanliga frågor om CEIP .

Överst på sidan

Windows Defender

Windows Defender söker efter skadlig kod och andra program som du förmodligen inte vill ha på datorn. Det innehåller funktionerna Microsoft Active Protection Service och Historik.

Microsoft Active Protection Service

Vad kan jag göra med den här funktionen?

Microsoft Active Protection Service (MAPS) är en frivillig grupp med deltagare i hela världen, däribland användare av Windows Defender. De försöker komma till rätta med skadlig kod. Via MAPS kan användarna skicka information om skadlig kod och annan oönskad programvara till

Microsoft i en rapport. MAPS kan skydda datorn genom att ladda ned nya signaturer för nyligen identifierad skadlig kod automatiskt.

Information som samlas in, bearbetas eller överförs

MAPS-rapporterna innehåller information om filer med potentiellt skadlig kod, t.ex. filnamn, kryptografiska hashvärden, programutgivare, filstorlekar och datumstämplingar. Dessutom kan MAPS samla in fullständiga webbadresser som visar varifrån filerna kom. Dessa webbadresser kan ibland innehålla personlig information, t.ex. sökord eller data som anges i formulär. Rapporterna kan dessutom omfatta de åtgärder du vidtog när Windows Defender meddelade dig att ett potentiellt oönskat program identifierades. MAPS tar med alla dessa uppgifter för att hjälpa Microsoft att bedöma hur effektivt Windows Defender är på att identifiera och ta bort skadlig kod och annan önskad programvara, och för att försöka identifiera ny skadlig kod.

Rapporterna skickas automatiskt till Microsoft när:

- Windows Defender identifierar program som ännu inte har riskanalyserats.
- Windows Defender identifierar ändringar i datorn av program som ännu inte har riskanalyserats.
- Windows Defender vidtar en åtgärd mot skadlig kod när den identifieras (som ett led i den automatiska justeringen).
- Windows Defender kör en schemalagd genomsökning och vidtar åtgärder på programvara som upptäcks baserat på dina inställningar.

Du kan gå med i MAPS med grundläggande eller avancerat medlemskap. Om du väljer att aktivera MAPS när du installerar Windows blir du grundmedlem. Rapporterna från grundmedlemmar innehåller den information som beskrivs i det här avsnittet. Rapporterna från avancerade medlemmar

är mer omfattande och kan ibland innehålla personlig information exempelvis från filsökvägar och partiella minnesdumpar. Dessa rapporter jämte rapporter från andra användare av Windows Defender som deltar i MAPS hjälper våra tekniker att upptäcka nya hot snabbare. Därefter skapas definitioner av skadlig kod, och sedan görs dessa uppdaterade definitioner tillgängliga för alla användare via Windows Update.

Om du går med i MAPS med grundläggande eller avancerat medlemskap:

- kan Microsoft begära att få en exempelrapport. Den här rapporten innehåller specifika filer från datorn som Microsoft misstänker kan vara oönskad programvara. Exempelrapporten används för vidare analys. Du får en fråga varje gång om du vill skicka exempelrapporten till Microsoft.

- Om Windows Update inte har lyckats ladda ned uppdaterade signaturer till Windows Defender under en viss tid, försöker Windows Defender använda MAPS för att ladda ned signaturer från en alternativ nedladdningsplats.

Den information du skickar till MAPS krypteras med SSL för att skydda din integritet.

Användning av informationen

Rapporter som skickas till MAPS används för att förbättra Microsofts program och tjänster. Rapporterna kan även användas för statistiska syften, testsyften eller analyser, samt för att skapa definitioner. MAPS samlar inte avsiktligt in någon personlig information. Om MAPS råkar samla in någon personlig information kommer Microsoft inte att använda den för att identifiera dig, kontakta dig eller rikta reklam mot dig.

Val och kontroll

Om du väljer standardinställningarna när du konfigurerar Windows aktiveras MAPS. Om du väljer anpassade

inställningar kan du ställa in MAPS genom att välja **Gå med i MAPS (Microsoft Active Protection Service) och hjälp Microsoft att agera mot skadliga appar och skadlig kod** under **Skicka info till Microsoft så att vi kan förbättra Windows och apparna**. När du har konfigurerat Windows kan du byta medlemskap i MAPS eller ändra inställningarna, och även inaktivera MAPS, på Verktyg-menyn i Windows Defender.

Historikfunktionen

Vad kan jag göra med den här funktionen?

Historikfunktionen ger tillgång till en lista över alla appar på datorn som Windows Defender identifierar och de åtgärder som vidtogs när apparna identifierades.

Dessutom kan du se en lista över appar som Windows Defender inte övervakar när de körs på datorn (de kallas tillåtna objekt). Dessutom kan du se appar som Windows Defender hindrar från att köras tills du väljer att ta bort dem eller tillåter dem att köras igen (de kallas objekt i karantän).

Information som samlas in, bearbetas eller överförs

Listan över program som Windows Defender identifierar, de åtgärder som du och andra användare vidtar samt de åtgärder som Windows Defender vidtar sparas automatiskt på datorn. Alla användare kan se igenom historien i Windows Defender och se skadlig kod och annan oönskad programvara som har försökt installera sig eller köras på datorn, eller som någon annan användare har tillåtit köras. Om du t.ex. får nys om ny skadlig kod, kan du titta igenom historiken och se om Windows Defender har hindrat den från att infektera datorn. Ingen information skickas till Microsoft.

Val och kontroll

En administratör kan ta bort historiklistorna.

Överst på sidan

Windows Felrapportering

Vad kan jag göra med den här funktionen?

Windows Felrapportering hjälper Microsoft och Microsofts partner att diagnostisera problem med de program du använder och tillhandahålla lösningar. Alla problem har inte lösningar, men när lösningar finns tillgängliga får du ett detaljerat lösningsförslag för ett problem som du har rapporterat eller tillgång till uppdateringar som du kan installera. För att förhindra problem och göra programvaran mer pålitlig ingår en del lösningar också i Service Pack och framtida programversioner.

Information som samlas in, bearbetas eller överförs

Många program är designade för att fungera ihop med Windows Felrapportering. Om ett problem uppstår i någon av dessa produkter, kan du få en fråga om du vill rapportera det.

Windows Felrapportering samlar in information som är till nytta för att diagnostisera och lösa ett problem som har inträffat, t.ex. var problemet förekom i programmet eller maskinvaran, hur allvarligt problemet är, filer som beskriver problemet, grundläggande information om program och maskinvara eller möjliga problem med programs prestanda och kompatibilitet. Om du använder Windows som värd för virtuella datorer kan felrapporterna som skickas till Microsoft innehålla information om dem.

Windows Felrapportering samlar även in information om appar, drivrutiner och enheter för att hjälpa Microsoft att förstå och förbättra appars och enheters kompatibilitet. Informationen om en app kan omfatta namnet på appens körbara filer. Informationen om enheter och drivrutiner kan omfatta namnet på enheterna du har installerat i datorn och de körbara filer som är kopplade till dessa enheters drivrutiner. Information om företaget som publicerade en app eller drivrutin kan samlas in.

Om du väljer att aktivera automatiska rapporter när du

ställer in Windows skickar rapporttjänsten automatiskt grundinformation om var problem uppträder. Vissa felrapporter kan oavsiktligt innehålla personlig information. En rapport som t.ex. innehåller en ögonblicksbild av datorminnet kan innehålla ditt namn, en del av ett dokument som du arbetar med eller data som du nyligen har skickat till en webbplats. Om det är troligt att en rapport innehåller information av den här typen, får du en fråga från Windows om du vill skicka dessa uppgifter även om du har aktiverat automatiska rapporter. Rapporter med filer och data kan lagras på datorn tills de skickas eller tas bort.

När du har skickat en rapport kan rapporteringstjänsten be dig om mer information om problemet som har uppstått. Om du väljer att ange ditt telefonnummer eller din e-postadress blir din felrapport personligt identifierbar. Microsoft kan kontakta dig och begära ytterligare information för att få hjälp med att lösa problemet som du har rapporterat.

Windows Felrapportering skapar slumpmässigt ett tal som kallas en GUID (globalt unik identifierare) som skickas till Microsoft med varje felrapport. GUID-värdet gör det möjligt för oss att fastställa vilken information som framöver ska skickas från en viss dator. GUID-värdet innehåller inte någon personlig information.

Information skickas krypterad via SSL för att skydda din integritet.

Användning av informationen

Microsoft använder information om fel och problem som rapporteras av Windows för att förbättra Microsofts produkter och tjänster liksom andra företags program och maskinvara som har designats för att användas med dessa produkter och tjänster. Vi använder GUID-värdet för att bestämma hur omfattande den feedback vi får är och hur den ska prioriteras. Med detta GUID kan Microsoft till exempel skilja mellan en kund som får samma problem

hundra gånger och hundra kunder som får samma problem en gång.

Microsofts anställda, underleverantörer, leverantörer och partner kan ges tillgång till relevanta delar av de uppgifter som samlas in, men de tillåts bara att använda informationen för att reparera eller förbättra Microsofts produkter och tjänster, eller andra företags program och maskinvara som har designats för att användas med Microsofts produkter och tjänster. Om en felrapport innehåller personlig information använder Microsoft den inte för att identifiera dig, kontakta dig eller rikta reklam mot dig. Men om du väljer att ange kontaktuppgifter enligt beskrivningen ovan, kan vi använda dem för att kontakta dig.

Val och kontroll

Om du väljer snabbinställningarna när du konfigurerar Windows skickar Windows Felrapportering automatiskt rapporter med grundinformation för att se om det finns någon lösning på problemen. Om du väljer anpassade inställningar kan du ställa in Windows Felrapportering genom att välja **Sök efter lösningar på problem med Windows Felrapportering** under **Sök efter lösningar på problem online**. Efter installationen av Windows kan du ändra inställningen i Åtgärdscenter på Kontrollpanelen.

Mer information finns online i sekretesspolicyn för Microsofts felrapporteringstjänst .

Överst på sidan

Windows Filassociation

Vad kan jag göra med den här funktionen?

Windows Filassociation hjälper användarna att associera filtyper till särskilda appar. Om du försöker öppna en filtyp och det inte finns någon app som har associerats till den, frågar Windows om du vill använda Windows Filassociation för att leta reda på en app till filen, vilket bland annat

omfattar att Windows Store söks igenom efter en kompatibel app. Appar som brukar associeras med filnamnstillägget visas.

Information som samlas in, bearbetas eller överförs

Om du väljer att använda Windows Filassociation skickas filnamnstillägget (t.ex. docx eller pdf) och datorns visningsspråk till Microsoft. Resten av filnamnet skickas inte till Microsoft. När en filassociation till en viss app skapas skickas en unik identifierare för appen för att identifiera varje filtyps standardapp.

Användning av informationen

När du skickar in ett filnamnstillägg returnerar tjänsten en lista över de appar som Microsoft vet kan öppna filer med det tillägget. Om du inte väljer att ladda ned och installera en app ändras ingen filtypsassociation.

Val och kontroll

När du försöker öppna en filtyp utan en associerad app, kan du välja om du vill använda Windows Filassociation. Ingen filassociationsinformation skickas till Microsoft såvida du inte väljer att använda tjänsten.

Överst på sidan

Windows Hjälp

Windows Hjälp och support online

Vad kan jag göra med den här funktionen?

Med Windows Hjälp och support online kan du – när funktionen är aktiv – få den senaste hjälpen och supporten när du är ansluten till Internet.

Information som samlas in, bearbetas eller överförs

Om du använder Windows Hjälp och support online skickas dina frågor till Microsoft och dina sökningar efter hjälpinnehåll när du klickar på en länk. Windows skickar viss information om datorns konfiguration för att försöka

hitta mer relevant hjälpinnehåll. Windows Hjälp och support online använder dessutom webbstandardtekniker som cookies.

Användning av informationen

Microsoft använder informationen för att returnera hjälpämnen som svar på sökfrågor, för att returnera de mest relevanta svaren samt för att förbättra befintligt innehåll. Vi använder informationen om datorns konfiguration för att visa hjälpinnehåll som lämpar sig för den. Vi använder cookies och andra webbtekniker för att göra det lättare att navigera i webbinnehållet och för att vi bättre ska förstå hur användarna utnyttjar Windows Hjälp online.

Val och kontroll

Hjälp och support online är aktiverat som standard. Om du vill ändra denna inställning trycker eller klickar du på ikonen **Inställningar** högst upp i fönstret Hjälp och support och markerar eller avmarkerar sedan **Få hjälp online**. Om du vill ta bort de cookies som används av Windows Hjälp öppnar du Internetalternativ på Kontrollpanelen, klickar eller trycker på knappen **Ta bort** under **Webbhistorik**, markerar **Cookies och webbplatsdata**och klickar eller trycker på **Ta bort**. Om du väljer att blockera alla cookies (i avsnittet Sekretess i Internetalternativ) sparar Windows Hjälp inga cookies.

Programmet för förbättring av hjälpfunktionen

Vad kan jag göra med den här funktionen?

Programmet för förbättring av hjälpfunktionen hjälper Microsoft att identifiera trender för hur våra kunder använder Windows Hjälp och support online så att vi kan förbättra sökresultaten och innehållets relevans.

Information som samlas in, bearbetas eller överförs

Programmet för förbättring av hjälpfunktionen skickar information till Microsoft om den version av Windows som

körs på datorn och hur du använder Windows Hjälp och support, däribland de sökfrågor som du skriver när du söker i Windows Hjälp och support och eventuella klassificeringar eller kommentarer om hjälpämnen som visas för dig. När du söker, bläddrar igenom eller klassificerar eller kommenterar hjälpämnena som visas för dig, skickas informationen till Microsoft.

HEIP skapar slumpmässigt ett tal som kallas en GUID (globalt unik identifierare) som skickas till Microsoft med varje HEIP-rapport. GUID-värdet gör det möjligt för oss att fastställa vilken information som skickas från en viss dator. GUID-värdet innehåller inte någon personlig information. GUID-värdet är inte detsamma som GUID-värdena som används i Windows Felrapportering eller Windows CEIP.

Användning av informationen

De data som samlas in används för att identifiera trender och användningsmönster så att Microsoft kan förbättra kvaliteten på innehållet vi tillhandahåller och sökresultatens relevans. Vi använder GUID-värdet för att bestämma hur omfattande de problem vi får reda på är och hur de ska prioriteras. Med detta GUID kan Microsoft till exempel skilja mellan en kund som upplever ett problem hundra gånger och hundra kunder som får samma problem en gång.

Ingen information som kan användas för att identifiera dig samlas avsiktligt in genom programmet för förbättring av hjälpfunktionen. Om du skriver in sådana uppgifter i sök- eller kommentarsrutorna skickas de visserligen, men Microsoft använder inte dem eller liknande information för att identifiera, kontakta eller rikta reklam till dig.

Val och kontroll

Om du väljer standardinställningarna när du installerar Windows går du automatiskt med i programmet för förbättring av hjälpfunktionen (Help Experience Improvement Program). Om du väljer att anpassa inställningar kan du ställa in inställningarna för programmet för förbättring av hjälpfunktionen genom att markera **Hjälp**

till att göra hjälpinnehållet i Windows ännu bättre genom att skicka info till programmet för förbättring av hjälpfunktionen under **Skicka info till Microsoft så att vi kan förbättra Windows och apparna**. Efter installationen av Windows kan du ändra inställningen i Windows Hjälp och support.

Överst på sidan

Fjärrhjälp

Vad kan jag göra med den här funktionen?

Du kan använda Fjärrhjälp om du vill bjuda in någon att ansluta till datorn och hjälpa dig med ett datorproblem, även om personen inte är i närheten. När anslutningen är gjord kan den andra personen se vad som händer på din dator. Om du tillåter det kan personen använda sin mus och sitt tangentbord för att styra din dator och visa hur du åtgärdar ett problem.

Information som samlas in, bearbetas eller överförs

Fjärrhjälp skapar en krypterad anslutning mellan de två datorerna via Internet eller det lokala nätverket. När någon ansluter till din dator med hjälp av Fjärrhjälp får den personen tillgång till skrivbordet och alla öppna dokument, däribland all synlig personlig information. Om du dessutom tillåter att den andra personen fjärrstyr din dator med sin mus eller sitt tangentbord kan han eller hon t.ex. ta bort filer och ändra inställningar. När anslutningen har upprättats byter Fjärrhjälp ut kontaktuppgifter, däribland användarnamnet, datorns namn och profilbilden. Alla fjärrhjälpsanslutningar dokumenteras i en sessionsloggfil.

Användning av informationen

Informationen används för att upprätta en krypterad anslutning och för att ge den andra personen tillgång till skrivbordet. Ingen information skickas till Microsoft.

Val och kontroll

Innan du låter någon ansluta till datorn ska du stänga alla öppna program och dokument som du inte vill visa för den som hjälper dig. Tryck på Esc om du vill avsluta sessionen därför att du på något sätt känner att dig olustig över vad personen ser eller gör på datorn. Du kan inaktivera sessionsloggning och utbytet av kontaktuppgifter genom att avmarkera dessa alternativ i inställningar för Fjärrhjälp.

Överst på sidan

Windows Search

Vad kan jag göra med den här funktionen?

Windows Search är ett snabbt och konsekvent sätt att söka efter appar, inställningar, filer eller innehåll i appar.

Information som samlas in, bearbetas eller överförs

När du använder Windows Search skickas de tecken du skriver i sökfältet (när du skriver dem) och den färdiga sökfrågan bara till Windows och den eventuella app som du söker i, så att Windows eller appen kan ge sökförslag och visa sökresultat. Windows lagrar sökfrågor och data om hur ofta du söker i apparna.

Användning av informationen

Windows använder de tidigare lagrade sökningarna för att ge sökförslag i rutan Sök. Informationen som lagras om hur ofta du söker i apparna används för att sortera listan över sökbara appar i frekvensordning i sökrutan. Om du söker i ett externt företags app bestäms bruket av informationen som samlas in av företagets sekretesspolicy. Om du söker i en app från Microsoft förklaras dess sekretesspolicy i ett separat dokument.

Val och kontroll

Windows lagrar dessa uppgifter som standard. Du kan inaktivera lagring av dessa uppgifter eller ta bort alla lagrade tidigare sökningar i Sök i Datorinställningar.

Överst på sidan

Windows Dela

Vad kan jag göra med den här funktionen?

Med Windows Dela kan du dela innehålla mellan olika Windows Store-appar som stöder delning. Du kan även dela innehåll med dina vänner.

Information som samlas in, bearbetas eller överförs

När du delar något överför källappen innehållet till målappen först när du har valt målet i rutan Dela. Om källappen inte har implementerat delning har du möjlighet att dela en bild av det som visas på skärmen. Målappar och personer som du delar innehåll med ofta visas i en lista i rutan Dela så att du når dem lättare. Ingen information skickas till Microsoft.

Användning av informationen

Informationen som lagras om hur ofta du delar med målappar och de personer som du ofta delar innehåll med används för att sortera listan i rutan Dela i frekvensordning. Om du delar information med ett externt företags app bestäms bruket av informationen som samlas in av företagets sekretesspolicy. Om du delar med en app från Microsoft förklaras dess sekretesspolicy i ett separat dokument.

Val och kontroll

Windows lagrar information om hur du använder Windows Dela som standard. Du kan inaktivera lagring av dessa uppgifter eller ta bort de lagrade målen i Dela i Datorinställningar.

Överst på sidan

Windows SmartScreen

Vad kan jag göra med den här funktionen?

Windows SmartScreen hjälper till att skydda datorn genom att undersöka filer och appar hos Microsoft innan du öppnar eller kör dem för att skydda dig mot eventuellt osäkra filer och appar. Windows frågar vad du vill göra innan en fil eller app som är okänd eller kanske osäker öppnas.

Information som samlas in, bearbetas eller överförs

Om du väljer att använda den här funktionen skickas information om vissa av apparna som du använder och vissa av filerna som du laddar ned från Internet till Microsoft. Informationen kan omfatta ett filnamn, en filidentifierare (ett ”hashvärde”) och information om ett digitalt certifikat jämte normal datorinformation och Windows SmartScreen-filtrets versionsnummer. Den information du skickar till Microsoft krypteras med SSL för att skydda din integritet.

Windows SmartScreen skapar slumpmässigt ett tal som kallas en GUID (globalt unik identifierare) som skickas till Microsoft med uppgifterna från SmartScreen. GUID-värdet gör det möjligt för oss att fastställa vilken information som skickas från en viss dator. GUID-värdet innehåller inte någon personlig information.

Användning av informationen

Microsoft använder informationen som beskrivs ovan för att varna dig om filer och appar som kan vara farliga. Vi använder också informationen till att analysera funktionens prestanda och till att förbättra kvaliteten på våra produkter och tjänster. Vi använder GUID-värdet för att bestämma hur omfattande den feedback vi får är och hur den ska prioriteras. Med detta GUID kan Microsoft till exempel skilja mellan en kund som får samma problem hundra gånger och hundra kunder som får samma problem en gång. Microsoft använder inte informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Om du väljer standardinställningarna när du installerar

Windows aktiveras Windows SmartScreen. Om du väljer att anpassa inställningar kan du ställa in Windows SmartScreen genom att markera **Använd Windows SmartScreen-filtret för att kontrollera filer och appar med Microsoft** under **Skydda din integritet och datorn**. Efter installationen av Windows kan du ändra inställningen i Åtgärdscenter på Kontrollpanelen.

Överst på sidan

Windows Taligenkänning

Vad kan jag göra med den här funktionen?

Windows Taligenkänning ger tillgång till taligenkänning i Windows och alla appar som väljer att utnyttja funktionen. Windows Taligenkänning förbättrar noggrannheten genom att lära sig hur du använder ditt språk, däribland vilka ljud och ord du brukar använda.

Information som samlas in, bearbetas eller överförs

Windows Taligenkänning lagrar en lista över ord och deras uttal på datorn. Ord och uttal läggs till i den här listan över hjälp av en ordlista och genom att du använder Windows Taligenkänning för att diktera och korrigera ord.

När Windows Taligenkännings funktion för dokumentgranskning är aktiverad, samlas text från Microsoft Office Word-dokument (med filnamnstillägget doc eller docx) och e-post (från andra e-postmappar än Borttaget eller Skräppost) in från datorn och från alla anslutna filresurser som finns med bland sökindexplatserna i Windows. Den sparas i fragment om ett, två eller tre ord. Fragment med ett ord omfattar enbart ord som du har lagt till i anpassade ordlistor och fragment med två eller tre ord omfattar bara ord som finns i standardordlistor.

All information som samlas in lagras i din standardprofil för tal på datorn. Talprofiler lagras för varje användare, och användarna kan inte komma åt andra användares profiler på datorn. Administratörer kan emellertid komma åt alla

profiler på datorn. Profilinformationen skickas inte till Microsoft om du inte väljer att skicka den när du får en fråga från Windows Taligenkänning. Du kan granska uppgifterna innan de skickas. Om du väljer att skicka informationen skickas även de data om akustisk anpassning som användes för att anpassa dina ljudegenskaper.

Om du slutför en taligenkänningssession, frågar Windows Taligenkänning dig om du vill skicka talprofilinformationen till Microsoft. Du kan granska informationen innan den skickas. Uppgifterna kan gälla inspelningar av din röst då du genomförde sessionen och annan information från din talprofil.

Användning av informationen

Windows Taligenkänning använder ord från talprofilen för att omvandla dina talade ord till text. Microsoft använder information från den personliga talprofilen för att förbättra sina program och tjänster. Vi använder inte informationen för att identifiera, kontakta eller skicka reklam till dig.

Val och kontroll

Du kan välja om du vill köra Windows Taligenkänning eller inte. Om du kör Windows Taligenkänning är dokumentgranskningsfunktionen aktiverad som standard. Du kan välja om du vill ändra dokumentgranskningsinställningarna den första gången du kör Windows Taligenkänning. Du kan ändra inställningarna för dokumentgranskning eller ta bort personliga talprofiler (och det mesta av uppgifterna om dokumentgranskning) genom att öppna Taligenkänning på Kontrollpanelen och klicka på **Avancerade talalternativ**. Du kan även använda alternativet Ändra befintliga ord i ordlistan och ta bort ord som du har lagt till i talprofilen. Men om du tar bort din personliga talprofil tas inte orden som har lagts till genom ordlistan bort.

Du kan välja de platser som dokumentgranskningsfunktionen hämtar ordfragment från genom att ändra platserna som ingår i Windows sökindex.

Öppna Indexeringsalternativ på Kontrollpanelen om du vill se eller ändra vilka platser som ingår i sökindexet i Windows.

I slutet av varje träningssession får du välja om du vill skicka träningsinformationen och annan profilinformation till Microsoft. Du kan även skicka information när Windows Taligenkänning startas genom att högerklicka på **Mikrofon**och sedan välja **Hjälp till att förbättra taligenkänning**. I bägge fallen kan du granska alla datafiler innan de skickas och kan välja att inte skicka dem.

Överst på sidan

Windows Store

I Windows Store kan du hitta, hantera och installera appar på datorn. Avsnitten nedan beskriver hur funktionerna i Store – och apparna som du laddar ned via Store – skulle kunna påverka din integritet och vad du kan göra för att kontrollera detta.

Store-appar och tjänsten

Vad kan jag göra med den här funktionen?

I Store kan du hitta och installera appar på datorn. Programmet håller även reda på vilka Store-appar som du har installerat, så att du kan ladda ned uppdateringar till dem och installera dem på fler än en dator.

Information som samlas in, bearbetas eller överförs

Om du vill hitta och installera appar måste du logga in i Store med ett Microsoft-konto. Det ger Store tillgång till information i din Microsoft-kontoprofil, t.ex. ditt namn, din e-postadress och din profilbild. Store samlar in och kopplar följande ytterligare information till ditt Store-konto:

- Betalningar till Store. Information om vad du har köpt, hur mycket och hur du betalade när du köpte appar eller gjorde köp via app med ditt Store-konto.

- Appar som du har installerat. Listan över appar som

du har installerat, licenspolicyn för varje app (permanent licens eller en tidsbegränsad provversion) och en lista över alla köp som du har gjort med ditt Store-konto i varje app. Utöver att lagra denna information på Internet i ditt Store-konto lagrar Store licensinformation på din dator för varje app som du installerar. Denna information visar att du äger licensen.

- Datorer som du har installerat appar på. Märket, modellen och datornamnet på varje dator som du installerar appar på jämte ett nummer som identifierar datorn unikt. Numret genereras utifrån datorns maskinvarukonfiguration och innehåller inte någon information om dig.

- Klassificeringar, recensioner och problemrapporter. När du har installerat en app kan du skriva en recension eller klassificera den i Store. Microsoft-kontot kopplas till dessa klassificeringar. Om du skriver en recension publiceras namnet och bilden från ditt Microsoft-konto med din recension.

- Store-inställningar. Inställningar som du väljer för att visa appar i Store, t.ex. om du bara vill visa appar som är tillgängliga på ditt modersmål.

Du kan välja att lagra dina betalningsuppgifter, t.ex. ditt kreditkortsnummer, i ditt Store-konto. Av säkerhetsskäl skickas den här informationen via SSL, och alla utom de sista fyra siffrorna i ditt kreditkortsnummer lagras krypterade.

Store samlar in viss information om ditt exemplar av Windows för att ta reda på om du köpte produkten från en butik, om det är ett utvärderingsexemplar, om du fick det genom ett volymlicensprogram eller om det installerades i förväg av en datortillverkare. Första gången du ansluter till Store skickas en lista över alla de appar som har förinstallerats på datorn till Store, som sedan kopplar licenser till dessa appar till ditt Store-konto.

En automatisk kontroll av om det finns några uppdateringar till apparna görs och du får ett meddelande när nya uppdateringar blir tillgängliga. Uppdateringar tillhandahålls genom att Store skickar följande uppgifter till Microsoft:

- En lista över samliga appar som har installerats från Store av alla användare av datorn
- Licensinformationen om varje app, däribland ägaren till varje licens
- Konfigurationsinställningarna för Windows Update och/eller Microsoft Update, t.ex. om du vill att uppdateringar ska laddas ned eller installeras automatiskt.
- Vad som lyckas, vad som misslyckas och de fel du stöter på när du uppdaterar appar från Store.
- En globalt unik identifierare (GUID) – ett genererat slumptal som inte innehåller någon personlig information. GUID-värden används för att identifiera enskilda datorer utan att identifiera användaren.
- Namnet på BIOS, dess versionsnummer och ändringsdatum – information om de nödvändiga programvarurutiner som testar maskinvaran, startar operativsystemet på datorn och överför data mellan maskinvaruenheterna som är anslutna till datorn.

När du tittar igenom Store och använder appar därifrån, samlar Microsoft in viss information så att vi ska förstå användningsmönster och trender, på ungefär samma sätt som många webbplatser analyserar sina besökares förehavanden. Inga av dessa aktivitetsdata används för att identifiera eller kontakta dig.

Användning av informationen

Microsoft använder dina kontaktuppgifter för att skicka dig de e-postmeddelanden som krävs för att tillhandahålla Store-tjänsterna, t.ex. kvitton för appar som du köper. Dina

betalningsuppgifter används så att du kan betala för det du köper; om du väljer att lagra den här informationen slipper du ange den varje gång. Microsoft använder uppgifterna om vad du har köpt för att sköta Store och ge kundsupport.

Store håller reda på alla appar som du har installerat. Du kan använda Store för att hantera listan över enheter som du har installerat appar på, och kundtjänsten kan även hjälpa dig att hantera dessa uppgifter. När du installerar en app visas den i köphistoriken i Store, även om du väljer att avinstallera den. Store använder den här listan för att se till att du inte kan installera appar på fler än ett visst antal enheter, enligt beskrivningen i användningsvillkoren för Windows Store. När du skriver en recension om en app, publiceras namnet och profilbilden som hör till ditt Windows-konto bredvid recensionen i Store. Om du rapporterar ett problem med en app får representanter för Store tillgång till rapporten för bedömning och åtgärd. De kan använda ditt namn och den e-postadress som hör till Store-kontot för att kontakta dig när de granskar rapporten, om det skulle visa sig vara nödvändigt.

Om de appar du har installerat har uppdaterats visas ett meddelande i Store, och antalet tillgängliga uppdateringar visas i Stores appanel. Du kan då se listan över tillgängliga uppdateringar och välja vilka du vill installera. Uppdaterade appar kan använda andra Windows-funktioner än tidigare, vilket skulle ge dem tillgång till andra resurser på datorn. Du kan se de ändrade listorna med funktioner på sidan Appbeskrivning. Det finns en länk dit från sidan med de tillgängliga uppdateringarna.

Store använder informationen som samlas in om ditt exemplar av Windows för att reda på hur Windows installerades på datorn (t.ex. om det var datortillverkaren som gjorde det i förväg). Med den här informationen kan Store ge dig tillgång till appar som tillverkaren bara erbjuder sina kunder. Uppgifterna används dessutom för att ge Microsoft information (och i avidentifierat skick även till tillverkaren, i vissa fall) om användningsmönster i Windows.

Microsoft använder vissa uppgifter om appköp och användningsdata i avidentifierat och samlat skick för att få reda på hur användarna utnyttjar Store (t.ex. hur användarna hittar apparna de installerar). Microsoft kan dela vissa av dessa samlade uppgifter med apputvecklare. Microsoft delar inga personliga uppgifter med apputvecklare. Vi använder de bläddrings- och användningsdata som samlas in av Store till att få en bättre förståelse av hur användarna utnyttjar Store och för att förbättra Stores funktioner och tjänster.

Val och kontroll

Om du väljer att använda Store skickas informationen som beskrivs i det här avsnittet till Microsoft enligt beskrivningen ovan.

Om du vill ta bort en recension som du har publicerat om en app ska du besöka appbeskrivningen i Store, redigera den och ta bort all text.

Store-appars behörighet

Vad kan jag göra med den här funktionen?

Många appar som du installerar från Windows Store är designade för att utnyttja särskild maskinvara och programfunktioner på datorn. Exempelvis kan en fotoapp behöva använda din webbkamera, och en restaurangguide kan behöva veta var du befinner dig för att kunna ge rekommendationer om restauranger i närheten.

Information som samlas in, bearbetas eller överförs

Här är en lista över funktioner som appar måste tala om att de använder:

- Din Internetanslutning. Tillåter apparna att ansluta till Internet.
- Inkommande anslutningar genom en brandvägg. Tillåter appen att skicka information till eller från din dator genom en brandvägg.
- Ett hem- eller arbetsplatsnätverk. Tillåter appen att

skicka information mellan din dator och andra datorer i samma nätverk

- Dina bilder, dina videor, din musik eller dina dokumentbibliotek. Tillåter appen att komma åt, ändra eller ta bort filer i dina bibliotek. Det gäller även åtkomst till eventuella andra data som är inbäddade i dessa filer, t.ex. platsinformation i foton.
- Flyttbart lagringsmedium. Tillåter appen att komma åt, lägga till, ändra eller ta bort filer på en extern hårddisk, ett USB-flashminne eller en bärbar enhet.
- Dina autentiseringsuppgifter i Windows. Tillåter appen att använda dina uppgifter för att autentisera dig och ge tillgång till ett företags intranät.
- Certifikat som lagras på datorn eller ett smartkort. Tillåter appen att använda certifikat för att ansluta säkert till organisationer som banker, myndigheter eller din arbetsgivare.
- Datorns textmeddelandefunktion. Tillåter appen att skicka och ta emot textmeddelanden.
- Din webbkamera och mikrofon. Tillåter appen att ta bilder och spela in ljud och video.
- Din plats. Tillåter appen att ta reda på ungefär var du befinner dig med hjälp av en GPS eller nätverksinformation.
- Datorns funktion för närkommunikation. Tillåter appen att ansluta till andra enheter i närheten som samma app körs på.
- Dina bärbara enheter. Tillåter appen att kommunicera med enheter som din mobiltelefon, digitalkamera eller bärbara musikspelare.
- Din information på en bärbar enhet. Tillåter appen att komma åt, lägga till, ändra eller ta bort kontakter,

kalendrar, uppgifter, anteckningar, statusar eller ringsignaler på din bärbara enhet.

- Ditt mobila bredbandskonto. Tillåter appen att hantera ditt mobila bredbandskonto.

Funktionerna som en app använder listas på appens beskrivningssida. Om du installerar en app tillåts den använda dessa funktioner, förutom din plats, dina textmeddelanden, webbkameran och mikrofonen, som anses extra känsliga. När en app begär åtkomst till en av dessa känsliga funktioner för första gången får du en fråga om du vill att appen ska få använda den. Du kan när som helst ändra dig angående detta.

Användning av informationen

Varje apps bruk av dessa funktioner är underställt utvecklarens sekretesspolicy. Om en app använder en av de känsliga funktionerna som beskrivs ovan, finns det en länk till apputgivarens sekretesspolicy på appens beskrivningssida i Store.

Val och kontroll

Du kan se vilka funktioner en app behöver i Store innan du installerar den. Windows frågar om du vill tillåta eller neka åtkomst till de mest känsliga av dessa funktioner – din plats, textmeddelanden, webbkameran och mikrofonen – första gången varje app använder dem.

När du läser igenom en apps beskrivningssida på Windows Store visas en förkortad lista över de funktioner som appen använder längst ned i den vänstra kolumnen. Den fullständiga listan finns på sidan Detaljer i appbeskrivningen. När du har installerat en app kan du se den fullständiga listan över de funktioner den använder när som helst och bestämma tillgången till de särskilt känsliga funktionerna. Gör detta genom att öppna appen, klicka eller trycka på snabbknappen Inställningar och sedan välja **Behörigheter**.

Hjälp till att förbättra Windows Store genom att skicka webbadresser till innehåll som appar använder

Vad kan jag göra med den här funktionen?

Vissa appar som du laddar ned från Store liknar webbplatser och kan utsätta datorn för program som kan vara farliga, t.ex. skadlig kod. Om du väljer att använda den här funktionen samlas information om webbinnehållet dessa appar använder in för att hjälpa Microsoft att diagnostisera beteende som kan vara farligt. Vi skulle t.ex. kunna använda informationen för att ta bort en app från Store.

Information som samlas in, bearbetas eller överförs

Om du väljer att skicka information om webbinnehållet som apparna använder samlar Microsoft in information om de webbadresser och det slags innehåll som dessa appar ansluter till när du använder dem. Det hjälper oss att identifiera vilka av apparna som tar emot innehåll från skadliga eller osäkra webbplatser. Rapporterna som skickas till Microsoft innehållet information såsom appens namn eller ID, de fullständiga webbadresserna som appen ansluter till och de fullständiga webbadresserna som indikerar platsen för eventuella JavaScript som appen ansluter till. Windows skapar slumpmässigt ett tal som kallas en GUID (globalt unik identifierare) som skickas till Microsoft med varje rapport. GUID-värdet gör det möjligt för oss att fastställa vilken information som framöver ska skickas från en viss dator. GUID-värdet innehåller ingen personlig information och används inte för att identifiera dig.

Den information du skickar till Microsoft krypteras för att skydda din integritet. Information som kan kopplas till en webbsida som apparna använder kan ingå, t.ex. sökvillkor och data som du har angett i apparna. Om du t.ex. slår upp ett ord i en ordlisteapp kan ordet kunna komma med i den information som skickas till Microsoft som en del av den

fullständiga adressen som appen hämtar. Microsoft filtrerar dessa adresser för att försöka ta bort personlig information när så är möjligt.

Användning av informationen

Microsoft ger regelbundet igenom informationen som skickas för att identifiera appar som kanske ansluter till farligt innehåll på webben, t.ex. skadliga webbadresser eller skript. Vi skulle kunna använda informationen till att vidta åtgärder mot t.ex. appar som kan vara skadliga. Adresser till webbinnehåll kan oavsiktligt innehålla personlig information, men den används inte för att identifiera, kontakta eller skicka reklam till dig. Vi använder GUID-värdet för att bestämma hur omfattande den feedback vi får är och hur den ska prioriteras. Med detta GUID kan Microsoft till exempel skilja mellan ett beteende som kan vara osäkert och som uppträder 100 gånger på en viss dator och samma beteende som inträffar en gång på 100 datorer.

Val och kontroll

Om du väljer snabbinställningarna när du konfigurerar Windows skickar Windows information om webbinnehållet som används av dina appar från Store som är uppbyggda med JavaScript. Om du väljer anpassade inställningar kan du ställa in den här inställningen genom att välja **Hjälp till att göra Windows Store ännu bättre genom att skicka URL:er till webbinnehåll som appar använder** under **Skicka info till Microsoft så att vi kan förbättra Windows och apparna**. Efter installationen kan du ändra inställningen i Sekretess i Datorinställningar.

Överst på sidan

Tjänsten Windows Time

Vad kan jag göra med den här funktionen?

Tjänsten Windows Time synkroniserar automatiskt datorns klocka mot en tidsserver i ett nätverk.

Information som samlas in, bearbetas eller överförs

Tjänsten ansluter till en tidsserver via Internet eller i ett lokalt nätverk med NTP-standardprotokollet (Network Time Protocol). Som standard synkroniserar denna tjänst mot time.windows.com en gång i veckan. Ingen information utöver normal information om datorn skickas till tidsservern.

Användning av informationen

Windows Time använder informationen för att synkronisera den lokala datorns klocka automatiskt.

Val och kontroll

Tjänsten Windows Time är aktiverad som standard. Du kan inaktivera den här funktionen eller välja den tidskälla du föredrar i Datum och tid på Kontrollpanelen. Välj fliken Internettid och klicka på **Ändra inställningar**. Appar eller andra tjänster påverkas inte direkt av att tjänsten Windows Time stängs av, men utan en tillförlitlig tidskälla kan den lokala datorns klocka dra sig jämfört med andra datorer i nätverket eller på Internet. Appar och tjänster som är beroende av att klockan går rätt kanske kraschar eller slutar att fungera korrekt om tidsskillnaden är tillräckligt stor mellan datorer i nätverket.

Överst på sidan

Windows Felsökning

Vad kan jag göra med den här funktionen?

Med Windows Felsökning kan du diagnostisera och åtgärda vanliga datorproblem.

Information som samlas in, bearbetas eller överförs

När du har kört ett felsökningspaket sparas resultatet på datorn. Dessa resultat kan innehålla personlig information, t.ex. ditt användarnamn eller namnet på en tjänst. Med Windows Felsökning kan du söka efter lösningar på

problem i Windows Hjälp och Windows-grupper på nätet. Sökord som är kopplade till problemet skickas till Microsoft så att det ska gå att hitta en lösning. Om exempelvis din skrivare inte fungerar som den borde och du behöver hjälp, skickas orden ”skrivare”, ”skriva ut” och ”utskrift” till Microsoft.

Användning av informationen

Microsoft använder informationen som samlats in av Windows Felsökning för att hjälpa till med att lösa problem som våra användare råkar ut för.

Val och kontroll

Om du väljer snabbinställningarna vid installationen av Windows söker Windows Felsökning efter felsökningspaket på nätet som standard. Dessa ändringar går att ändra i Felsökning på Kontrollpanelen. Klicka på **Visa historik**, markera ett resultat och klicka sedan på **Ta bort**.

Överst på sidan

Microsoft

Sekretess

Aktuell information om Microsofts rutiner för databehandling finns i Microsofts sekretesspolicy. Här kan du också läsa om de senaste verktygen vi tillhandahåller för att du ska få tillgång till och kontrollera dina data, och hur du kontaktar oss om du har frågor om sekretess.

Sekretesspolicy för Windows 8 och Windows Server 2012

På den här sidan

Senast uppdaterad: **augusti 2012**

Den här sidan är ett tillägg till Sekretesspolicy för Windows 8 och Windows Server 2012 (”Windows sekretesspolicy”). Sekretesspolicyn innehåller fyra avsnitt:

- Snabböversikt
- Policyn, som är fullständig sekretesspolicy för Windows , vilken innehåller länkar till Windows-funktioner som har egna policyer
- Funktioner (tillägg), som beskriver de funktioner som påverkar sekretessen i Windows 8 och Windows Server 2012
- Server (tillägg) (det här dokumentet) som beskriver de ytterligare funktioner som påverkar sekretessen i Windows Server 2012

För att förstå de rutiner för insamling och användning av data som är relevanta för en viss funktion eller tjänst i Windows, ska du läsa den fullständiga sekretesspolicyn för Windows och

Felrapportering (WER)

eventuella tillägg. Dessutom bör du läsa detta white paper för administratörer.

Loggning av användaråtkomst (UAL)

Det här gör funktionen

Loggning av användaråtkomst samlar in och sammanställer poster med klientförfrågningar för serverroller (både användar- och enhetsbegäranden) och installerade produkter (som har registrerats med Loggning av användaråtkomst) på den lokala servern. Dessa data, i form av IP-adresser, användarnamn och i vissa fall värdnamn och/eller id:n för virtuella datorer, lagras i lokala ESE-databaser (Extensible Storage Engine) och är endast tillgängliga för administratörer. För UAL används en WMIv2-provider och tillhörande Windows PowerShell-cmdletar för att hämta användaråtkomstdata som är avsedda för hantering av kunders berättigande av klientåtkomstlicenser offline, där faktiska poster med unika klientbegäranden är viktiga.

Information som samlas in, behandlas eller överförs

IP-adresser, användarnamn, och i vissa fall värdnamn (om DNS-rollen har installerats), samt id:n för virtuella datorer (om Hyper-V-rollen har installerats) samlas in lokalt på servern när Loggning av användardata är aktiverat. Inga insamlade data skickas till Microsoft.

Användning av information

UAL-data görs tillgängliga för administratörer via lokala ESE-databaser, WMI-providern och Windows PowerShell-cmdletar. Windows använder inte dessa data utanför själva UAL-funktionen.

Val och kontroll

UAL är aktiverat som standard. UAL-tjänsten kan stoppas och startas medan servern körs. Om du vill inaktivera UAL permanent öppnar du Windows PowerShell, skriver Disable-UAL och startar om servern. En administratör kan ta bort alla historiska data som samlats in genom att först stoppa tjänsten, inaktivera UAL och sedan ta bort alla filer i mappen %SystemRoot%\System32\LogFiles\SUM\.

Överst på sidan

Serverhanteraren

Det här gör funktionen

Serverhanteraren är ett hanteringsverktyg som gör att en administratör kan övervaka en eller flera servrar och visa allmän eller rollspecifik status för att utföra hanteringsaktiviteter och komma åt andra serverhanteringsverktyg.

Information som samlas in, behandlas eller överförs

Serverhanteraren samlar in följande typer av information från en server som administratören hanterar:

- **Allmän serverinformation:** NetBios-namn och fullständigt domännamn (FQDN), kontoautentiseringsuppgifter som anges i ”Hantera som”-funktionen, IPv4-adress, IPv6-adress, hanterbarhetsstatus, beskrivning, version av operativsystemet, typ, senaste uppdateringen, processorer, minne, klusternamn, klusterobjekttyp, aktiveringsstatus, SKU, operativsystemets arkitektur, tillverkare, CEIP-konfiguration (Customer Experience Improvement Program) och konfiguration av Windows Felrapportering (WER).

- **Händelser:** ID, allvarlighetsgrad, källa, logg, datum och tid för varje händelse från Windows och andra loggar som administratören väljer.

- **Alla tjänster:** namn, status och starttyp.

- **Information om serverroll:** BPA-resultat (Best Practice Analyzer) för roller som är installerade på servern.

- **Prestandainformation:** exempel för prestandaräknare och meddelanden om processoranvändning och ledigt minne.

Användning av information

Den här informationen lagras i Serverhanteraren och skickas inte till Microsoft. Den visas i Serverhanteraren för att hjälpa

administratörer att övervaka system.

Val och kontroll

En administratör kan välja eller välja bort insamling av data från en server, förutom den lokala servern, genom att lägga till eller ta bort servern i Serverhanteraren. En administratör kan uttryckligen tillhandahålla autentiseringsuppgifter för anslutning till en fjärrserver. Serverhanteraren ber administratören uttryckligen om tillåtelse att lagra autentiseringsuppgifterna lokalt i Serverhanteraren och administratören kan när som helst ta bort dessa autentiseringsuppgifter.

Överst på sidan

Active Directory Federation Services (AD FS)

Det här gör funktionen

Active Directory Federation Services (AD FS) är en företagslösning med federation och enkel inloggning för lokala eller andra nätverksbaserade program. Med AD FS kan administratörer ge användarna möjlighet att samarbeta mellan organisationer och enkelt komma åt program på lokala nätverk eller andra nätverk samtidigt som säkerheten upprätthålls. AD FS använder en säkerhetstokentjänst som använder Active Directory Domain Services (AD DS) för att autentisera användare och utfärda säkerhetstoken med olika protokoll. Denna token signeras digitalt och innehåller anspråk om användaren som kommer från AD DS, Lightweight Directory Access Protocol (LDAP), SQL Server eller ett anpassat arkiv, eller från en kombination av dessa.

Information som samlas in, behandlas eller överförs

En användares autentiseringsuppgifter samlas in när användaren autentiseras med AD FS. Autentiseringsuppgifterna skickas direkt till Active Directory Domain Services för autentisering och AD FS sparar dem inte lokalt. Användarens attribut i Active Directory Domain Services kan användas för att generera utgående anspråk, beroende på vilka anspråksregler AD FS-administratören har konfigurerat. Utgående anspråk skickas till tillförlitliga partner som en AD FS-administratör har upprättat en förtroenderelation

med. Ingen information skickas till Microsoft.

Användning av information

Microsoft har inte tillgång till denna information. Den här informationen är endast avsedd att användas av kunden.

Val och kontroll

Använd AD FS om du vill att AD FS ska samla in eller skicka data till betrodda partner.

Överst på sidan

IP-adresshantering

Det här gör funktionen

IP-adresshantering (IPAM) gör att serveradministratörer kan spåra IP-adresser, värdnamn och klient-ID:n (till exempel MAC-adressen i IPv4 och DUID i IPv6) för datorer eller enheter i ett nätverk med användarens inloggningsuppgifter.

Information som samlas in, behandlas eller överförs

IPAM-servern samlar in granskningsloggar och händelser från DHCP-servrar, domänkontrollanter och nätverksprincipservrar och lagrar sedan IP-adressen, värdnamnet, klientidentifieraren och användarnamnet lokalt för den inloggade användaren. En serveradministratör kan söka i de insamlade loggarna baserat på IP-adress, klientidentifierare, värdnamn och användarnamn med IPAM-konsolen. Ingen del av den här informationen skickas till Microsoft.

Användning av information

Microsoft har inte tillgång till denna information. Den här informationen är endast avsedd att användas av kunden.

Val och kontroll

IPAM installeras inte som standard och måste installeras av serveradministratören. När IPAM har installerats aktiveras automatiskt granskning av IP-adresser. Om du vill inaktivera granskning av IP-adresser på en server som IPAM har installerats på startar du Schemaläggaren på IPAM-servern, bläddrar till Audit

Task under Microsoft\Windows\IPAM och inaktiverar aktiviteten.

Överst på sidan

Enhetlig fjärråtkomst

Det här gör funktionen

Enhetlig fjärråtkomst gör att fjärranvändare kan ansluta till ett privat nätverk, till exempel ett företagsnätverk, via Internet. Enhetlig fjärråtkomst använder DirectAccess för att förse fjärrklientdatorer som kör Windows 8 med en avbrottsfri och transparent anslutning till företagsnätverk. Den tillhandahåller också fjärråtkomst (RAS) som är traditionella VPN-tjänster, inklusive plats-till-plats-anslutning, lokal anslutning eller annan nätverksanslutning.

Information som samlas in, behandlas eller överförs

Vid användaröverväkning med Enhetlig fjärråtkomst lagrar DirectAccess-servern information om fjärranvändare som ansluter till det privata nätverket. Detta omfattar information som värdnamnet för fjärranvändaren, användarnamnet för Active Directory och den offentliga IP-adressen för fjärrklienten (om klienten finns bakom NAT (Network Address Translation) är detta den offentliga IP-adressen). Den här informationen kan också lagras i den interna Windows-databasen (WID)/RADIUS-servrar (endast med administratörens medgivande). Endast en DirectAccess-administratör (en domänanvändare med ett lokalt administratörskonto) kan komma åt och visa informationen.

Användning av information

Den här informationen används av administratören för att felsöka klientanslutningen och används även i gransknings- eller regelefterlevnadssyfte. Ingen information skickas till Microsoft.

Val och kontroll

Fjärrklientövervakning är aktiverat som standard och kan inte inaktiveras. Övervakningsdata lagras i WID/RADIUS-servrar endast om en administratör har konfigurerat redovisning så att något av dessa alternativ används. Om en administratör inte har

konfigurerat redovisning lagras ingen information. En administratör kan också konfigurera redovisning på en fjärråtkomstserver så att användarnamn och IP-adressinformation inte lagras.

Överst på sidan

Fjärrskrivbordstjänster (RDS)

Det här gör funktionen

Fjärrskrivbordstjänster ger företag en plattform för att implementera en centraliserad skrivbordsstrategi, hantera skrivbord och program, och förbättra flexibiliteten och regelefterlevnaden samtidigt som datasäkerheten förbättras.

Information som samlas in, behandlas eller överförs

Vid RDS-användaröverväkning lagrar värdservern för fjärrskrivbordssessionen information om fjärranvändare som ansluter till RDS-resurser. Detta omfattar information som värdnamnet för fjärranvändaren, användarnamnet för Active Directory och den offentliga IP-adressen för fjärrklienten (om klienten finns bakom NAT (Network Address Translation) är detta den offentliga IP-adressen). Dessa data lagras automatiskt i den interna Windows-databasen (WID)/SQL-servrar när användarna ansluter. Ingen information skickas till Microsoft. Endast domänanvändare med ett lokalt administratörskonto kan komma åt och visa informationen.

Användning av information

Den här informationen används av administratören för att felsöka klientanslutningen. Den används även internt i granskning- eller regelefterlevnadssyfte. Ingen information skickas till Microsoft.

Val och kontroll

Klientövervakning är aktiverat som standard och kan inte inaktiveras. Övervakningsinformationen lagras i WID/SQL-servern.

Överst på sidan

Windows Customer Experience Improvement Program (CEIP) och Windows Felrapportering (WER)

Det här gör funktionen

Mer information om de här funktionerna finns på fliken Funktioner (tillägg) eller detta white paper för administratörer.

Information som samlas in, behandlas eller överförs

Om du vill veta mer om specifik information som samlas in, bearbetas och överförs via dess funktioner kan du läsa om CEIP och WER på fliken Funktioner (tillägg) .

Användning av information

Om du vill veta hur vi använder den information som samlas in av dessa funktioner kan du läsa om CEIP och WER på fliken Funktioner (tillägg) .

Val och kontroll

CEIP är inaktiverat som standard och WER frågar dig som standard innan felrapporter skickas till Microsoft. Du kan aktivera eller inaktivera CEIP i Serverhanteraren, på Kontrollpanelen och med kommandoradsmetoder. WER kan endast ställas in med kommandoradsmetoder.

Om du vill aktivera eller inaktivera CEIP via Kontrollpanelen klickar du på **System och underhåll** och klickar sedan på **Problemrapporter och -lösningar**. Under Se även i det vänstra fönstret klickar du sedan på **Inställningar för Programmet för kvalitetsförbättring** för att aktivera eller inaktivera CEIP.

Kontroller i Serverhanteraren

Lokal server

- Aktivera CEIP
  Öppna Serverhanteraren och välj **Lokal server**. Klicka på länken Customer Experience Improvement Program, markera **Ja, jag vill delta i Customer Experience Improvement Program** i dialogrutan och klicka sedan på **OK.**

- Inaktivera CEIP
  Öppna Serverhanteraren och välj **Lokal server**. Klicka på länken Customer Experience Improvement Program, markera **Nej, jag vill inte delta** i dialogrutan och klicka sedan på **OK.**

- Aktivera WER
  Öppna Serverhanteraren och välj **Lokal server**. Klicka på länken Windows Felrapportering, markera **Ja, skicka sammanfattningsrapporter automatiskt** och klicka sedan på **OK**.

- Inaktivera WER
  Öppna Serverhanteraren och välj **Lokal server**. Klicka på länken Windows Felrapportering, markera **Jag vill inte delta och fråga inte igen** och klicka sedan på **OK**.

Flera datorer

- Aktivera CEIP
  Öppna Serverhanteraren och välj **Alla servrar**. Markera alla servrar på panelen Servrar (Ctrl+A), högerklicka och välj **Konfigurera Windows Automatisk feedback** . På fliken Customer Experience Improvement Program markerar du **Ja, jag vill delta (rekommenderas)**. Använd den här inställningen för alla servrar genom att markera kryssrutan bredvid servernamnet på kontrollen Välj servrar och klicka sedan på **OK**.

- Inaktivera CEIP
  Öppna Serverhanteraren och välj Alla servrar. Markera alla servrar på panelen Servrar (Ctrl+A), högerklicka och välj **Konfigurera Windows Automatisk feedback** . På fliken Customer Experience Improvement Program markerar du **Nej, jag vill inte delta**. Använd den här inställningen för alla servrar genom att markera kryssrutan bredvid servernamnet på kontrollen Välj servrar och klicka sedan på **OK.**

- Aktivera WER
  Öppna Serverhanteraren och välj **Alla servrar**. Markera alla servrar på panelen Servrar (Ctrl+A), högerklicka och välj

Konfigurera Windows Automatisk feedback . På fliken Windows Felrapportering markerar du **Ja, skicka sammanfattningsrapporter automatiskt (rekommenderas)**. Använd den här inställningen för alla servrar genom att markera kryssrutan bredvid servernamnet på kontrollen Välj servrar och klicka sedan på **OK**.

- Inaktivera WER
  Öppna Serverhanteraren och välj **Alla servrar**. Markera alla servrar på panelen Servrar (Ctrl+A), högerklicka och välj **Konfigurera Windows Automatisk feedback** . På fliken Windows Felrapportering markerar du **Nej, jag vill inte delta**. Använd den här inställningen för alla servrar genom att markera kryssrutan bredvid servernamnet på kontrollen Välj servrar och klicka sedan på **OK**.

Överst på sidan

Microsoft

Sekretess

Sekretess hos Microsoft

Dina data är privata på jobbet, hemma och på resande fot.

På Microsoft värdesätter vi och skyddar sekretess. Vi tror på transparens, så att människor och organisationer kan kontrollera sina data och ha meningsfulla val i hur de används. Vi stärker och skyddar sekretessvalen för varje person som använder våra produkter och tjänster.

Hemma

Sekretess är i centrum för hur vi utformar de produkter och tjänster som kunderna använder varje dag. Vi tillhandahåller sekretessresurser och kontroller så att du kan hantera dina data och hur de används.

Besök sekretesspanelen □

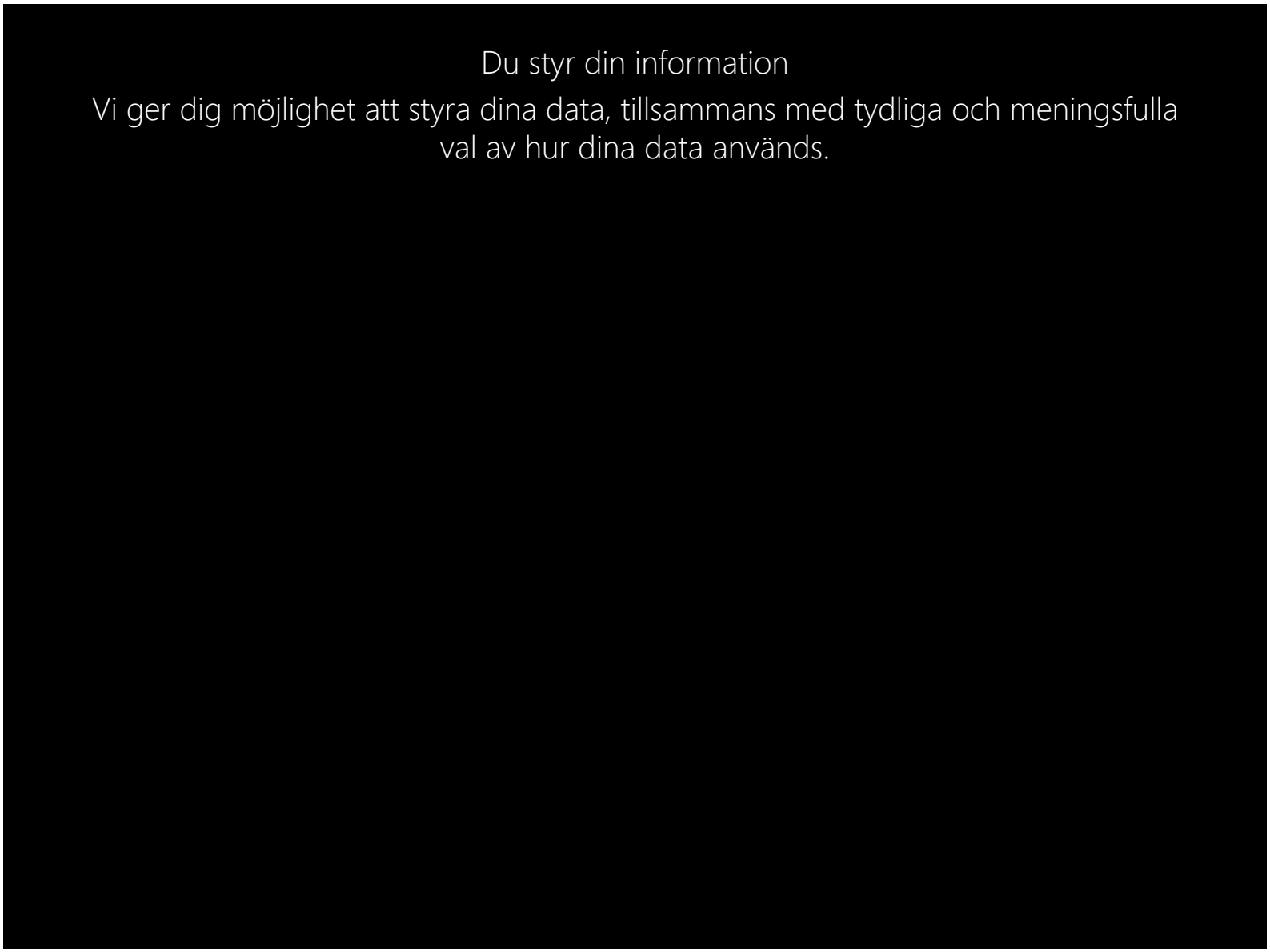
På jobbet

För enterprise- och företagskunder, IT-administratörer eller alla som använder Microsoft-produkter på jobbet går du till Microsoft Trust Center för att få information om sekretess och säkerhetsmetoder i våra produkter och tjänster.

Besök Microsoft Trust Center □

Vårt sekretessåtagande

Vi har grundat våra sekretessåtaganden i starka datastyrningsmetoder, så att du kan lita på att vi skyddar sekretessen och konfidentialiteten för dina data och endast använder dem på ett sätt som överensstämmer med de skäl som du angav.

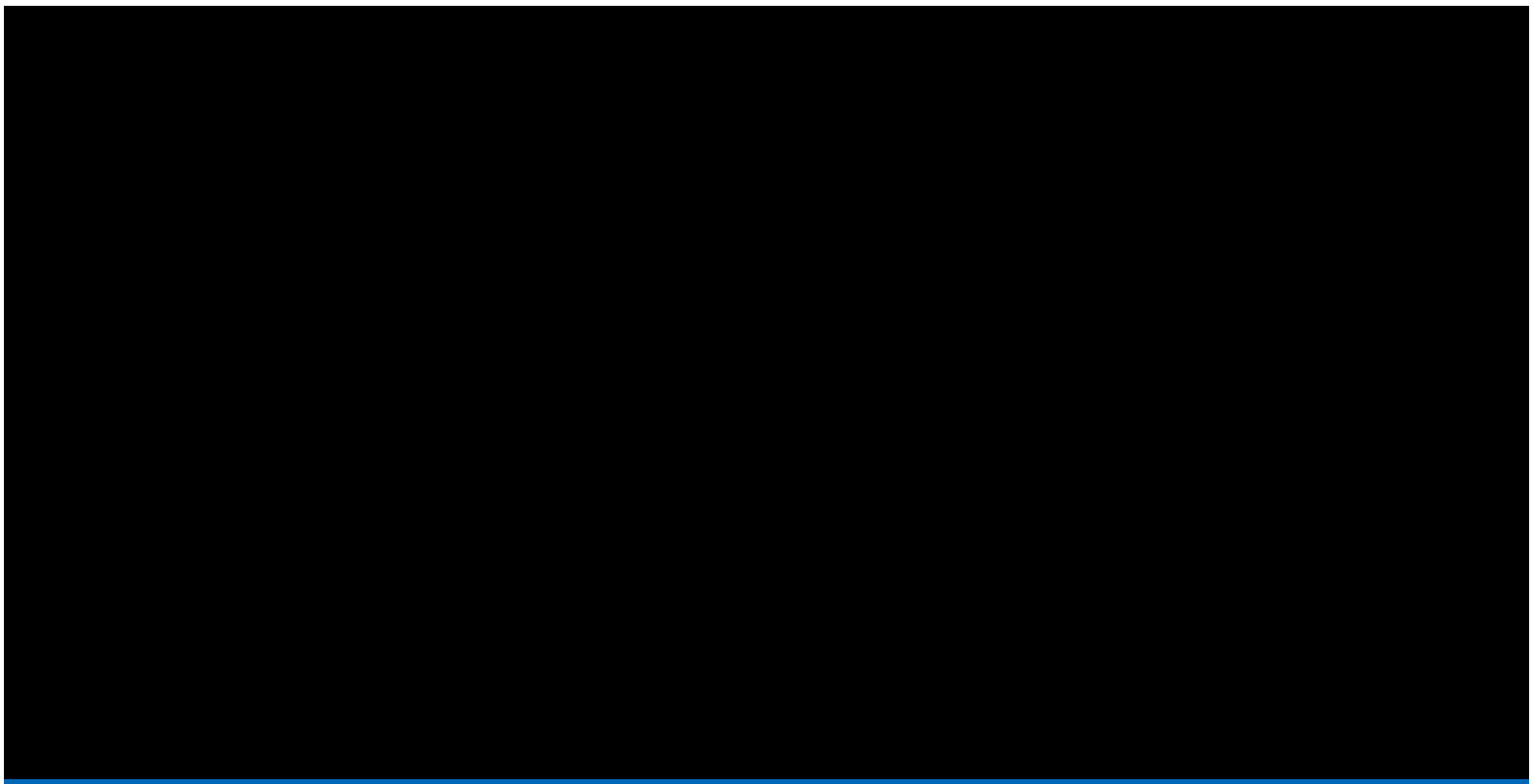


Dina data är skyddade

Vi skyddar dina data noggrant med hjälp av kryptering och andra rekommenderade säkerhetsmetoder.

Du kan förvänta dig sekretess efter design

Vi utformar våra produkter med ett kärnåtagande för att upprätthålla användarsekretessen.



Vi står upp för dina rättigheter

Vi bekämpar starkare sekretesslagar och -skydd och skyddar dina rättigheter om en myndighetsbegäran görs för data.

Dessa principer utgör grunden för Microsofts inställning till dataintegritet och fortsätter forma hur vi bygger våra produkter och tjänster.

Få mer information om hur vi använder dessa principer i praktiken.

- Vi publicerar regelbundet Microsofts sekretessrapport för att hålla dig uppdaterad om vårt sekretessarbete.
- Vi förklarar hur kunder kan exportera eller ta bort personliga data i Vanliga frågor och svar om sekretess.
- Vi erbjuder detaljerad sekretessinformation om våra produkter och tjänster i Microsofts sekretesspolicy.
- Vi anser att tekniken vi skapar bör vara till nytta för alla på jorden och för själva planeten. Gå till Microsofts sociala åtaganden för mer information.

Sekretesspanelen Microsoft Trust Center

Microsofts sekretessrapport

Informationsförfrågningar från myndigheter

Nyheter

Kolla in de senaste artiklarna, blogginläggen och nyheterna från Microsoft om hur du skyddar din integritet hemma och på jobbet. (En del innehåll kanske bara är tillgängligt på engelska.)

Förbättra sekretessen på arbetsplatsen med Microsoft Priva

Microsoft Priva är en ny sekretesslösning som utformats för att hjälpa organisationer att skapa integritetskänsliga arbetsplatser och ge informationsarbetare möjlighet att fatta beslut om smart datahantering.

Läs mer om Microsofts sekretesspolicy □

Microsoft strävar efter en viktig ny milstolpe för dataskydd

Europeiska unionen och U.S. Government presenterade nyligen det nya Trans-Atlantic Data Privacy Framework, ett avtal som utformats för att bygga upp och stärka dataskyddsbryggorna mellan EU och USA. Microsoft uppskattar den här viktiga milstolpen.

Läs Julie Brills blogginlägg om dataavtalet □

EU-datagräns för Microsoft Cloud: En förloppsrapport

Läs om den viktiga milstolpen i vår resa mot att skapa EU:s datagräns för Microsoft Cloud och vårt kontinuerliga åtagande att ge kunderna robust insyn i våra metoder och framsteg mot implementeringen av EU:s datagräns.

Läs förloppsrapporten för EU:s datagräns □

Skydda vår datainfrastruktur genom några nya metoder för sekretess

Frågan som det offentliga samhället, företag, akademiska myndigheter och myndigheter bör ställa sig är inte om vi kan använda data, utan snarare hur vi kan aktivera ansvarsfull dataanvändning för att skapa en bättre värld och skydda grundläggande mänskliga rättigheter. Läs om hur vi' utforskar utvecklingen av nya metoder där det behövs för att möjliggöra ansvarsfull användning och delning av data.

Läs mer om nya metoder för sekretess

Mer information om hur du hanterar dina sekretessinställningar finns i Var hittar jag sekretessinställningar i Microsoft-produkter?

Om du bor i delstaten Kalifornien kan du läsa vårt meddelande om California Consumer Privacy Act (CCPA) för konsumenter i Kalifornien.

Vi arbetar alltid att bli bättre, så om du märker att något i våra produkter eller tjänster inte fungerar som du förväntar dig när det gäller sekretess, får du gärna meddela oss.

- Surface Laptop Go 2
- Surface Pro 8
- Surface Laptop Studio
- Surface Pro X
- Surface Go 3
- Surface Pro 7+
- Microsoft 365
- Windows 11-appar

- Kontoprofil
- Download Center
- Microsoft Store-support
- Returer
- Orderspårning
- Återvinning
- Kommersiella garantier

- Microsoft Education
- Enheter för utbildning
- Microsoft Teams för utbildning
- Microsoft 365 Education
- Office Education
- Utbildning och utveckling för lärare
- Erbjudanden för elever och föräldrar
- Azure för studenter

Företag

- Microsoft Cloud
- Microsoft Security
- Azure
- Dynamics 365
- Microsoft 365
- Microsoft Advertising
- Microsoft Industry
- Microsoft Teams

Utvecklare och IT

- Utvecklarcenter
- Dokumentation
- Microsoft Learn
- Microsoft Tech Community
- Azure Marketplace
- AppSource
- Microsoft Power Platform
- Visual Studio

Företag

- Karriärmöjligheter
- Om Microsoft
- Företagsnyheter
- Sekretess på Microsoft
- Investerare
- Hållbarhet

Microsoft

Sekretess

Aktuell information om Microsofts rutiner för databehandling finns i Microsofts sekretesspolicy. Här kan du också läsa om de senaste verktygen vi tillhandahåller för att du ska få tillgång till och kontrollera dina data, och hur du kontaktar oss om du har frågor om sekretess.

Sekretesspolicy för Windows 8 och Windows Server 2012

Senast uppdaterad: **augusti 2012**

I den här snabböversikten över den fullständiga Sekretesspolicy för Windows 8 och Windows Server 2012 sekretesspolicyn (”Windows sekretesspolicy”) beskrivs några av rutinerna för insamling och användning av data i Windows 8 och Windows Server 2012 (”Windows”). Den här informationen fokuserar på funktioner som kommunicerar med Internet och är inte avsedd att vara en fullständig beskrivning. Den gäller inte för andra webbplatser, produkter eller tjänster från Microsoft, varken i online- eller offlineversioner.

Den här sekretesspolicyn innehåller fyra avsnitt:

- Snabböversikt (den här sidan)
- Policyn, det vill säga den fullständiga sekretesspolicyn för Windows som innehåller länkar till Windows-funktioner, som i sin tur har egna policyer
- Funktioner (tillägg), som beskriver de funktioner som påverkar sekretessen i Windows 8 och Windows Server 2012

- Server (tillägg), som beskriver de ytterligare funktioner som påverkar sekretessen i Windows Server 2012

Mer information om hur du kan skydda din dator, din personliga information och din familj på Internet finns på Microsofts säkerhetscenter.

Din information

- Vissa Windows-funktioner kan be om ditt tillstånd att samla in eller använda information från din dator, inklusive personlig information. Windows använder den här informationen på det sätt som anges i den fullständiga Windows sekretesspolicy, i Funktioner (tillägg) och i Server (tillägg).
- Vissa Windows-funktioner kan, med ditt medgivande, dela personlig information via Internet.
- Om du väljer att registrera programvaran blir du ombedd att uppge personlig information.
- Anledningen till att Windows måste aktiveras är att vi vill minska piratkopieringen och säkerställa att våra kunder får den programvarukvalitet de förväntar sig. Vid aktiveringen skickas viss information om din dator till Microsoft.
- Du kan välja att logga in på Windows med ett Microsoft-konto. Det gör att du kan synkronisera Windows-inställningar och logga in automatiskt på appar och webbplatser. När du skapar ett Microsoft-konto blir du ombedd att ange personlig information.
- Ytterligare information

Överst på sidan

Dina alternativ

- I Windows finns flera sätt att ställa in hur informationsöverföringen via Internet ska fungera för Windows-funktioner. Mer information om hur du ställer in dessa funktioner finns i avsnitten Funktioner (tillägg) och

Server (tillägg).

- Vissa funktioner som använder Internet är aktiverade som standard för att göra upplevelsen bättre.
- Ytterligare information

Överst på sidan

Användning av information

- Vi använder den insamlade informationen till att aktivera de funktioner som du använder och tillhandahålla tjänster som du begärt. Vi använder också den också till att förbättra våra produkter och tjänster. För att kunna tillhandahålla våra tjänster uppger vi ibland information till andra företag som arbetar åt oss. Endast företag som behöver informationen i arbetssyfte har åtkomst till den. Dessa företag måste hålla denna information konfidentiell och får inte använda informationen i något annat syfte.
- Ytterligare information

Överst på sidan

Kontakta oss

Mer information om våra sekretessrutiner finns i den fullständiga Windows sekretesspolicy. Du kan också skriva till oss via vårt webbformulär.

Överst på sidan

Microsoft

Privacy

Privacy Frequently Asked Questions (FAQs)

What are Data Subject Rights (DSRs)?

Microsoft is committed to giving customers transparency and control over their data. Data Subject Rights (DSRs) are the rights that individuals (or "data subjects") have to view, correct, export, and delete personal data that companies hold about them. We have built controls into our products and services so you can see what personal data Microsoft has collected and you can make choices about that data.

What personal data does Microsoft collect about me?

Microsoft collects data to help you do more. To do this, we use the data we collect to provide, improve, and develop our products and services, and to provide you with personalized experiences.

If you use products like Outlook.com, Skype, OneDrive, or Xbox, you likely have a personal Microsoft account. To access and delete data associated with these products, you can sign in to your account.

You can learn more about Microsoft and your privacy at privacy.microsoft.com. If you would like more detailed information about the data we collect, you can review the 'Personal data we collect' section of the Microsoft Privacy Statement.

How can I view and download personal data Microsoft holds about me?

At Microsoft, we believe privacy starts with putting you in control of your data. Your privacy dashboard is the place where you can view and clear data that Microsoft saves to the cloud. This data includes your browsing and Bing search history, location data, apps and services activity, and more.

If you would like to view and update profile, contact, and security info, you can sign in to your

Microsoft account.

If you have personal content that you want to view or download from Microsoft products, you can find tools within those products.

- **Bing search history:** View and export your search history on your privacy dashboard or within your Bing settings
- **OneDrive:** View and download your files in OneDrive
- **Outlook.com:** Export your emails, calendar, and contacts in your Outlook.com Settings>General>Privacy and data. Learn more: Import and export Outlook email, contacts, and calendar
- **Skype:** Export your Skype chat history and files
- **Xbox:** Some data is available to view and edit by accessing My Xbox on the Xbox console or on the Xbox.com website

To access other data related to your Microsoft account, you can contact our privacy team. If you are having trouble signing in to your account, see Get help with your Microsoft account.

How can I delete my personal data?

We understand that you may want to delete personal data that Microsoft has collected. Your privacy dashboard is the place where you can view and clear data that Microsoft saves to the cloud. This data includes your browsing and Bing search history, location data, apps and services activity, and more.

If you would like to update and remove profile, contact, and security info, you can sign in to your Microsoft account. To close your Microsoft account and delete the data in the account, see How to close your Microsoft account.

If you have personal content that you want to delete from Microsoft products, you can find tools within those products.

- **Bing search history:** Delete your search history on your privacy dashboard or within your Bing settings
- **Bing content or search results relating to you:** Report a concern to Bing via the Bing webform
- **OneDrive:** Delete your files in OneDrive

- **Outlook.com:** Delete your emails, calendar, and contacts at Outlook.com Learn more: Delete email in Outlook.com
- **Skype:** Delete chats and conversations within your Skype app. Learn more: How do I remove an instant message or clear a conversation in Skype?
- **Xbox:** Some data is available to delete by accessing My Xbox on the Xbox console or on the Xbox.com website

To delete other data related to your Microsoft account, you can contact our privacy team. If you are having trouble signing in to your account, see Get help with your Microsoft account.

I'm a child or teenager. What choices do I have about my data?

At Microsoft, we care about protecting the privacy and safety of young people online.

Depending on your age and where you live, you may need permission from a parent or guardian to create a Microsoft account. Your parent or guardian may also be asked to create a Microsoft family group.

Once you have an account, you can make choices about the data we get and how we use it. For example,

- You can access and delete some of your data through the Microsoft privacy dashboard. Depending on your age and where you live, you may need parental permission to delete your data.
- You can choose whether to receive certain messages from Microsoft.
- Many of our products offer other privacy settings and controls that you can use.

You can find privacy and family safety information on our Privacy for young people page. Complete privacy information can be found on the Microsoft Privacy Statement.

You can contact us about more ways to access or control your personal data. The best way to contact us is by using our web form.

I don't have a Microsoft account. Can I still find out what personal data Microsoft holds about me?

Yes. If you are looking to view or delete personal data that is not linked to an existing Microsoft account, our privacy team is happy to assist. This may be data collected outside of a logged-in Microsoft account experience, for example, an email address you provided as part of attending an event or using an app. You can submit a request for personal data linked to an email address and other identifiers by contacting our privacy team.

I use Microsoft products at work or school. How can I view and delete personal data collected through my use of Microsoft products at work or school?

In many cases, data collected in relation to your work or school account is owned and controlled by your organization. You should work with your IT administrator for questions related to this data. You can learn more in the 'Products provided by your organization-notice to end users' and 'Enterprise and developer products' sections of the Microsoft Privacy Statement.

How can I limit the personal data Microsoft collects?

Our products and services offer a number of controls and resources to enable our users to configure the level of privacy appropriate for them. You can manage many of these settings on your privacy dashboard. There you can view, download and clear the most meaningful data tied to your Microsoft account including browse, search history, precise location data, and more. You can also manage apps and services that have permission to access certain data connected to your Microsoft account, choose whether to see interest-based advertising, and update your communications preferences. For Windows users, we have also published detailed information on diagnostic data collection and how you can update your collection settings.

To learn more about how to configure your privacy settings in Microsoft products and services, see our help article: Where can I find privacy settings in Microsoft products?

How can I opt out of personalized advertising?

Some of Microsoft's services are supported by advertising. To show ads you're more likely to be interested in, we use data like your location, Bing searches, Microsoft or advertiser web pages you view, demographics, and things you've favorited. We don't use what you say in email, chat, video calls or voice mail, or your documents, photos or other personal files to target ads to you.

You can opt out of personalized advertising on Microsoft sites and services by visiting the Ads

settings page on your privacy dashboard. Please note that this option will not prevent you from seeing ads but means the ads you see will be randomized and may not be of interest to you.

How can I opt out of promotional communications from Microsoft?

You can choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. If you have a personal Microsoft account, you can manage your communications preferences on your privacy dashboard. If you do not have a personal Microsoft account, you can manage your Microsoft email contact preferences by using this web form.

Who do I contact if I have more questions?

If you have a privacy concern, request, or question, please contact our privacy team. We will respond to questions or concerns as required by law and within a period no longer than 30 days.

If you live in the EU or are a EU citizen, you can also contact the Microsoft EU Data Protection Officer at: Microsoft Ireland Operations Limited, Attn: Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland. Telephone: +353 1 706 3117.

Microsoft

Privacy

Privacy at Microsoft

Your data is private at work, at home, and on the go.

At Microsoft, we value, protect, and defend privacy. We believe in transparency, so that people and organizations can control their data and have meaningful choices in how it is used. We empower and defend the privacy choices of every person who uses our products and services.

At home

Privacy is at the center of how we shape the products and services that customers use every day. We provide privacy resources and controls, so you can manage your data and how it is used.

Visit the privacy dashboard

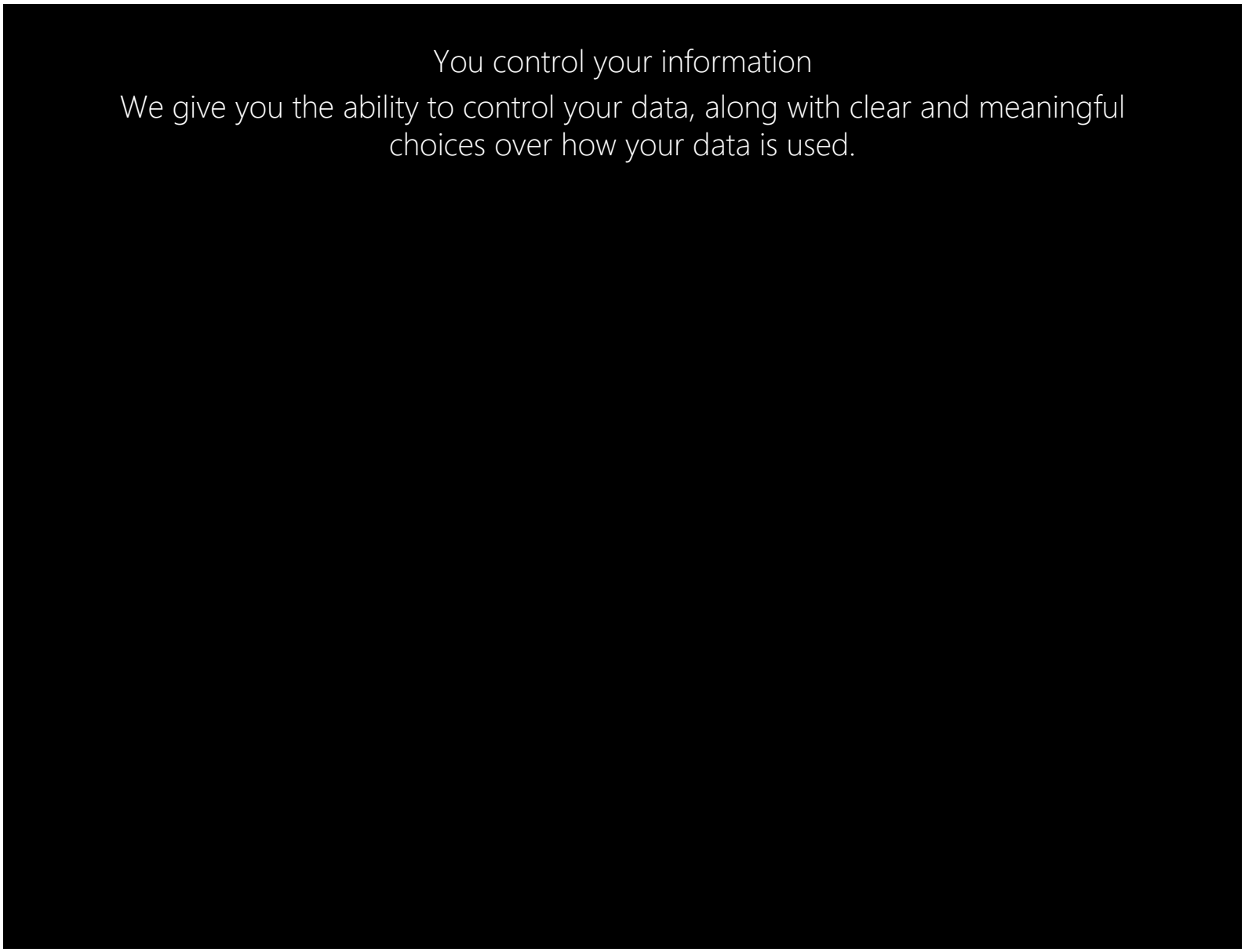
At work

For enterprise and business customers, IT admins, or anyone using Microsoft products at work, visit the Microsoft Trust Center to get information about privacy and security practices in our products and services.

Visit Microsoft Trust Center □

Our commitment to privacy

We ground our privacy commitments in strong data governance practices, so you can trust that we'll protect the privacy and confidentiality of your data and will only use it in a way that's consistent with the reasons you provided it.

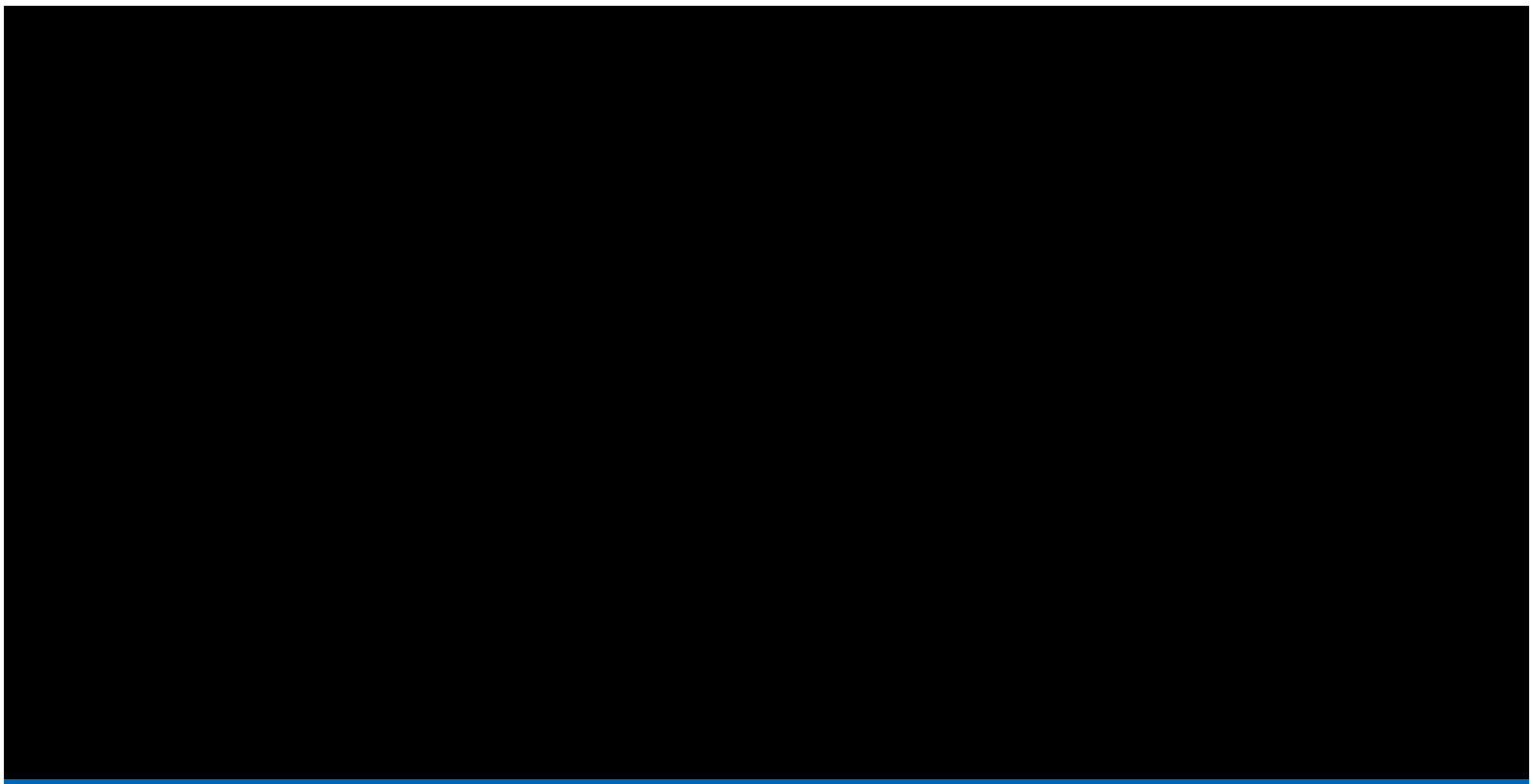


Your data is protected

We rigorously protect your data using encryption and other security best practices.

You can expect privacy by design

We design our products with a core commitment to uphold user privacy.



We stand up for your rights

We fight for stronger privacy laws and protections, and will protect your rights if a government request is made for data.

These principles form the foundation of the Microsoft approach to privacy and will continue to shape the way we build our products and services.

Get more information about how we put those principles into practice.

- We regularly publish the Microsoft Privacy Report to keep you updated about our privacy work.
- We explain how customers can export or delete personal data in our Privacy FAQs.
- We offer in-depth privacy information about our products and services in the Microsoft Privacy Statement.
- We believe that the technology we create should benefit everyone on the planet, and the planet itself. Visit the Microsoft Corporate Social Responsibility for more information.

Privacy dashboard Microsoft Trust Center

Microsoft Privacy Report Government information requests

What's new

Check out the latest articles, blog posts, and news from Microsoft about protecting your privacy at home and at work. (Some content might only be available in English.)

Improve workplace privacy with Microsoft Priva

Microsoft Priva is a new privacy solution designed to help organizations build privacy-resilient workplaces, and empower information workers to make smart data-handling decisions.

Learn more about Microsoft Priva □

Microsoft committed to important new milestone for data protection

The European Commission and the U.S. government recently announced the new Trans-Atlantic Data Privacy Framework, an agreement designed to rebuild and strengthen the data protection bridge between the EU and the U.S. Microsoft applauds this important milestone.

Read Julie Brill's blog post about the data agreement

EU Data Boundary for the Microsoft Cloud: A progress report

Read about the important milestone in our journey toward creating the EU Data Boundary for the Microsoft Cloud, and our ongoing commitment to provide customers with robust transparency about our practices and progress toward the implementation of the EU Data Boundary.

Read the EU Data Boundary progress report □

Protecting our data infrastructure through some new approaches to privacy

The question civil society, business, academics and governments should be asking is not if we can use data but rather how we can enable responsible data use to create a better world and protect fundamental human rights. Read about how we're exploring the development of new approaches where needed to enable the responsible use and sharing of data.

Read more about new approaches to privacy □

To learn about managing your privacy settings, see Where can I find privacy settings in Microsoft products?

If you are a resident of the state of California, please see our California Consumer Privacy Act (CCPA) Notice for California Consumers.

We're always working to improve, so if you notice something in our products and services that doesn't work the way you'd expect when it comes to privacy, please let us know.

Diagnostics, feedback, and privacy in Windows

Privacy, Windows 11, Windows 10

Together, diagnostics and feedback are how you and your Windows device tell Microsoft what's really going on.

As you use Windows, we collect diagnostic information, and to make sure we're listening to you, our customer, we've also built ways for you to send us feedback anytime, and at specific times, like when Windows asks you a question about how something is working for you.

Note: Microsoft is increasing transparency by categorizing the data we collect as *required* or *optional*. Windows 10 is in the process of updating devices to reflect this new categorization, and during this transition Basic diagnostic data will be recategorized as Required diagnostic data and Full diagnostic data will be recategorized as Optional diagnostic data.

What data is collected and why

Microsoft uses diagnostic data to keep Windows secure and up to date, troubleshoot problems, and make product improvements as described in more detail below. Regardless of whether you choose to send Optional diagnostic data, your device will be just as secure and will operate normally. This data is transmitted to Microsoft and stored with one or more unique identifiers that can help us recognize an individual user on an individual device and understand the device's service issues and use patterns.

- **Required** diagnostic data is information about your device, its settings and

capabilities, and whether it is performing properly. This is the minimum level of diagnostic data needed to help keep your device reliable, secure, and operating normally.

- **Optional** diagnostic data includes additional details about your device and its settings, capabilities, and device health. Optional diagnostic data also includes information about the websites you browse, device activity (sometimes referred to as usage), and enhanced error reporting. Optional diagnostic data can also include the memory state of your device when a system or app crash occurs (which may unintentionally include parts of a file you were using when a problem occurred). Required diagnostic data will always be included when you choose to send Optional diagnostic data. While your device will be just as secure and operate normally when only sending Required diagnostic data, the additional information we collect when you've chosen to send Optional diagnostic data makes it easier for us to identify and fix issues and make product improvements that benefit all Windows customers.

Some of the data described above may not be collected from your device even if you choose to send Optional diagnostic data. Microsoft minimizes the volume of Optional diagnostic data we collect from all devices by collecting some of the data from only a small percentage of devices (sample). By running Diagnostic Data Viewer, you can see an icon which indicates whether your device is part of a sample and also which specific data is collected from your device. Instructions for how to download the Diagnostic Data Viewer tool can be found in Windows 10 at **Start** □ > **Settings** □ > **Privacy** □ > **Diagnostics & feedback** and in Windows 11 at **Start** □ > **Settings** □ > **Privacy & security** > **Diagnostics & feedback**.

Specific data items collected in Windows diagnostics are subject to change to give Microsoft flexibility to collect the data needed for the purposes described. For example, to ensure Microsoft can troubleshoot the latest performance issue impacting users' computing experience or update a Windows device that is new to the market, Microsoft may need to collect data items that were not collected previously. For a current list of data types collected for Required diagnostic data and Optional diagnostic data, see Windows Required diagnostic events and fields and Windows Optional diagnostic data.

We use **Required** diagnostic data to keep Windows devices up to date. Microsoft uses:

- Basic error information to help determine whether problems your device is experiencing can be addressed by the update process.
- Information about your device, its settings and capabilities, including applications and drivers installed on your device, to ascertain whether your device is ready for and compatible with the next operating system or app release and ready for update.
- Logging information from the update process itself to understand how well your device's updates are proceeding through the stages of downloading, pre-installation, post-installation, post-reboot, and setup.
- Data about the performance of updates on all Windows devices to assess the success of an update's deployment and to learn device characteristics (e.g., hardware, peripherals, settings, and applications) that are associated with the success or failure of an update.
- Data about which devices have had upgrade failures and why to determine whether to offer the same upgrade again.

We use both **Required** diagnostic data and **Optional** diagnostic data to troubleshoot issues to help keep Windows and related products and services reliable and secure.

Microsoft uses **Required** diagnostic data to:

- Comprehend the immense number of hardware, system, and software combinations customers use.
- Analyze issues based on specific hardware, system, and software combinations and identify where problems or issues occur with a specific or limited set of devices.
- Determine whether an app or process experiences a performance issue (e.g., the app crashes or hangs) and when a crash-dump file is created on the device (crash dumps themselves are not collected without additional permissions, such as choosing to send Optional diagnostic data).
- Understand the effectiveness and fix problems with the diagnostic transmission system itself.

Microsoft uses the additional data collected when you choose to send **Optional** diagnostic data to help spot and fix problems more quickly.

We use:

- Information about app activity to understand what the user was doing in an app that caused a problem in conjunction with what we learn about the impact of other apps or processes running on a device.
- Information about device health, such as battery level or how quickly applications respond to input, to better understand the data we collect about application performance issues and make corrections.
- Information contained in enhanced error reporting and crash dumps to better understand the data related to the specific conditions under which an error or crash occurred.

We use **Required** diagnostic data to improve Windows. We use **Optional** diagnostic data to improve Windows and related products and services.

Microsoft uses **Required** diagnostic data for product improvement in the context of keeping your Windows device up to date and secure; problem-solving; accessibility; reliability; performance; enhancing existing Windows features; compatibility of apps, drivers, and other utilities; privacy; and energy efficiency.

Microsoft uses **Required** diagnostic data for this purpose as follows:

- Information about customers' devices, peripherals, and settings (and their configurations) is used to prioritize product improvements by determining which improvements will have the greatest positive impact to the most Windows customers.
- Information about which apps are installed on devices is used to prioritize app-compatibility testing and feature improvements for the most popular apps.

Additional data collected when you choose to send **Optional** diagnostic data is used to help make even more meaningful improvements to Windows and related products and services:

- App activity information helps us prioritize app-compatibility testing and make feature improvements to apps and features that are used the most.
- Information about the impact of device characteristics, configuration, and app activity on device health (for example on battery life) is used to analyze and make changes that improve the performance of Windows devices.
- Aggregate information about browsing history in Microsoft browsers is used to tune Bing's search algorithms to provide more effective search results.

If your device is being managed by an organization's IT department, there may be additional changes to how your diagnostic data is managed on the group policies set on the device. See Configure Windows diagnostic data in your organization for more details. If an enterprise engages Microsoft to manage their devices, we will use diagnostic and error data for managing, monitoring, and troubleshooting the enterprise's devices.

If you choose to turn on **Tailored experiences**, we will use your Windows diagnostic data to offer you personalized tips, ads, and recommendations to enhance Microsoft experiences. If you have selected **Required** as your Diagnostic data setting, personalization is based on information about your device, its settings and capabilities, and whether it is performing properly. If you have selected **Optional**, personalization is also based on information about how you use apps and features, plus additional information about the health of your device. We do not use the content of crash dumps, websites you browse, speech, typing, or inking input data for personalization when we receive such data from customers who have selected **Optional**.

Tailored experiences include suggestions on how to customize and optimize Windows, as well as ads and recommendations for Microsoft and third-party products and services, features, apps, and hardware for your Windows experiences. For example, to help you get the most out of your device, we may tell you about features you may not know about or that are new. If you are having a problem with your Windows device, you may be offered a solution. You may be offered a chance to customize your lock screen with pictures, or to be shown more pictures of the kind you like, or fewer of the ones you don't. Or, if you are running out of space on your hard drive, Windows may recommend you try OneDrive or purchase hardware to gain more space.

If you choose to turn on the **Improve inking & typing** setting, Microsoft will collect samples of the content you type or write to improve features such as handwriting recognition, autocompletion, next word prediction and spelling

correction, and we use this data in the aggregate to improve the inking and typing feature for everyone who uses Windows. When Microsoft collects inking and typing diagnostic data, it is divided into small samples and processed to remove unique identifiers, sequencing information, and other data (such as email addresses and numeric values) which could be used to reconstruct the original content or associate the input to you. It also includes associated performance data, such as changes you manually make to text, as well as words you've added to the dictionary. This data is not used for Tailored experiences.

> **Note:** In previous versions of Windows, the **Improve inking & typing** setting is not available, and this data is collected when **Diagnostic data** is set to **Full** instead.

How to control your diagnostics and feedback settings

When you set up your Windows device for the first time, you can choose to send optional diagnostic data to Microsoft.

During setup, you can also choose whether or not you'd like **Tailored experiences** set to **On** or **Off**. On newer versions of Windows, you can choose whether or not you'd like **Improve inking & typing** set to **On** or **Off**.

If you decide you want to change these settings after you've completed Windows setup, follow the appropriate steps in the following sections.

To change the Diagnostic data setting

1. Do one of the following:

   - In Windows 10, go to **Start** □, then select **Settings** □ > **Privacy** > **Diagnostics & feedback**.

   - In Windows 11, go to **Start** □, then select **Settings** □ > **Privacy & security** > **Diagnostics & feedback**.

2. Under **Diagnostic data**, select the option you prefer. If the options are unavailable, you may be using a device managed by your workplace or

organization. In that case, you'll see **Some settings are hidden or managed by your organization** at the top of the Diagnostics & feedback screen.

Note: Windows also has other privacy settings that control whether app activity and browsing history data is sent to Microsoft, such as the Activity history setting.

To change the Tailored experiences setting

1. Do one of the following:
   - In Windows 10, go to **Start** □, then select **Settings** □ > **Privacy** > **Diagnostics & feedback**.
   - In Windows 11, go to **Start** □, then select **Settings** □ > **Privacy & security** > **Diagnostics & feedback**.
2. Under **Tailored experiences**, choose the setting you'd prefer.

To view your diagnostic data

You can view diagnostic data for your device in real time by using the Diagnostic Data Viewer. Note that you will only be able to view data that is available while the Diagnostic Data Viewer is running. The Diagnostic Data Viewer does not allow you to view your diagnostic data history.

In Windows 10:

- Go to **Start** □, then select **Settings** □ > **Privacy** > **Diagnostics & feedback**.
- Make sure that the **Diagnostic data viewer** setting is turned **On**, and then select **Diagnostic Data Viewer**.

In Windows 11:

- Go to **Start** □, then select **Settings** □ > **Privacy & security** > **Diagnostics**

& feedback.

- Make sure that the **View diagnostic data** setting is turned **On**, and then select **Open Diagnostic Data Viewer**.

To delete your diagnostic data

Under **Delete diagnostic data**, you can delete diagnostic data for your device. Note that selecting this option does not delete the diagnostic data that is associated with your Microsoft account, nor does it stop your diagnostic data from being sent to Microsoft. If your organization has enrolled the device to services that rely on this data, your IT department might have a copy of this device's diagnostic data.

1. Do one of the following:

   - In Windows 10, go to **Start** □, then select **Settings** □ > **Privacy** > **Diagnostics & feedback**.

   - In Windows 11, go to **Start** □, then select **Settings** □ > **Privacy & security** > **Diagnostics & feedback**.

2. Under **Delete diagnostic data**, select **Delete**.

To view and delete any additional diagnostic data associated with your Microsoft account, visit the Microsoft privacy dashboard.

To stop letting Microsoft use your typing and handwriting info to improve typing and writing services for all customers

1. Do one of the following:

   - In Windows 10, go to **Start** □, then select **Settings** □ > **Privacy** > **Diagnostics & feedback**.

   - In Windows 11, go to **Start** □, then select **Settings** □ > **Privacy & security** > **Diagnostics & feedback**.

2. Turn the **Improve inking and typing** setting **Off**.

To change how often we ask you for feedback

We will occasionally display a message asking you to rate or provide written feedback about the product or services you use. You can use the **Feedback frequency** setting to adjust how often we ask you for this feedback.

1. Do one of the following:

   - Go to **Start** □, then select **Settings** □ > **Privacy** > **Diagnostics & feedback**.

   - Go to **Start** □, then select **Settings** □ > **Privacy & security** > **Diagnostics & feedback**.

2. Under **Feedback frequency**, select the option you prefer.

To send us feedback at any time

1. Type **Feedback Hub** in the search bar.

2. Type some keywords from your issue in the box marked **Give us feedback to make Windows better** and press Enter.

3. If you find your issue, upvote it. If you don't find it, you can give new feedback by filling out the form.

□ SUBSCRIBE RSS FEEDS

Need more help?

Join the discussion

ASK THE COMMUNITY □

Get support

CONTACT US □

Was this information helpful? Yes No

Microsoft

Privacy

Privacy at Microsoft

Your data is private at work, at home, and on the go.

At Microsoft, we value, protect, and defend privacy. We believe in transparency, so that people and organizations can control their data and have meaningful choices in how it is used. We empower and defend the privacy choices of every person who uses our products and services.

At home

Privacy is at the center of how we shape the products and services that customers use every day. We provide privacy resources and controls, so you can manage your data and how it is used.

Visit the privacy dashboard

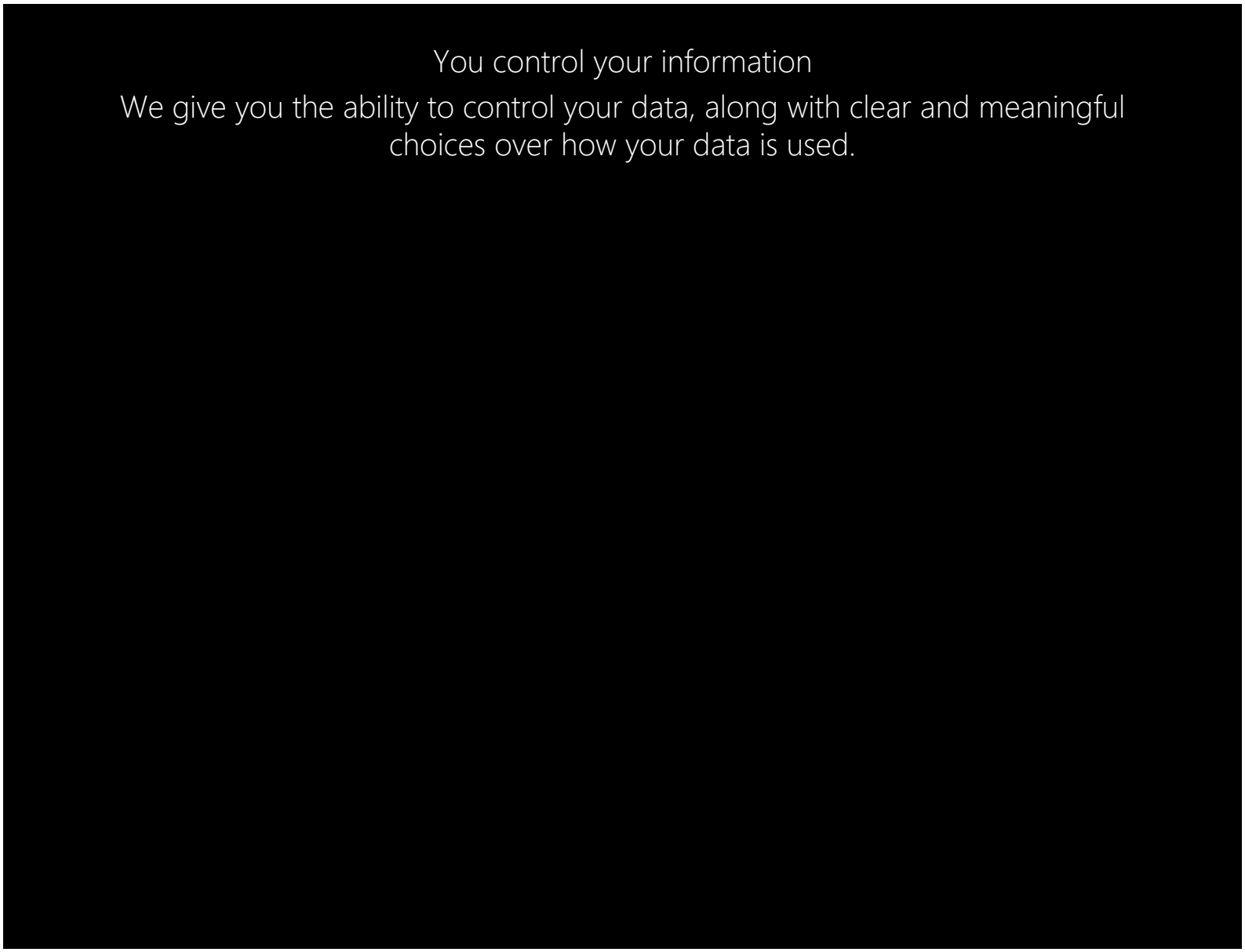
At work

For enterprise and business customers, IT admins, or anyone using Microsoft products at work, visit the Microsoft Trust Center to get information about privacy and security practices in our products and services.

Visit Microsoft Trust Center □

Our commitment to privacy

We ground our privacy commitments in strong data governance practices, so you can trust that we'll protect the privacy and confidentiality of your data and will only use it in a way that's consistent with the reasons you provided it.

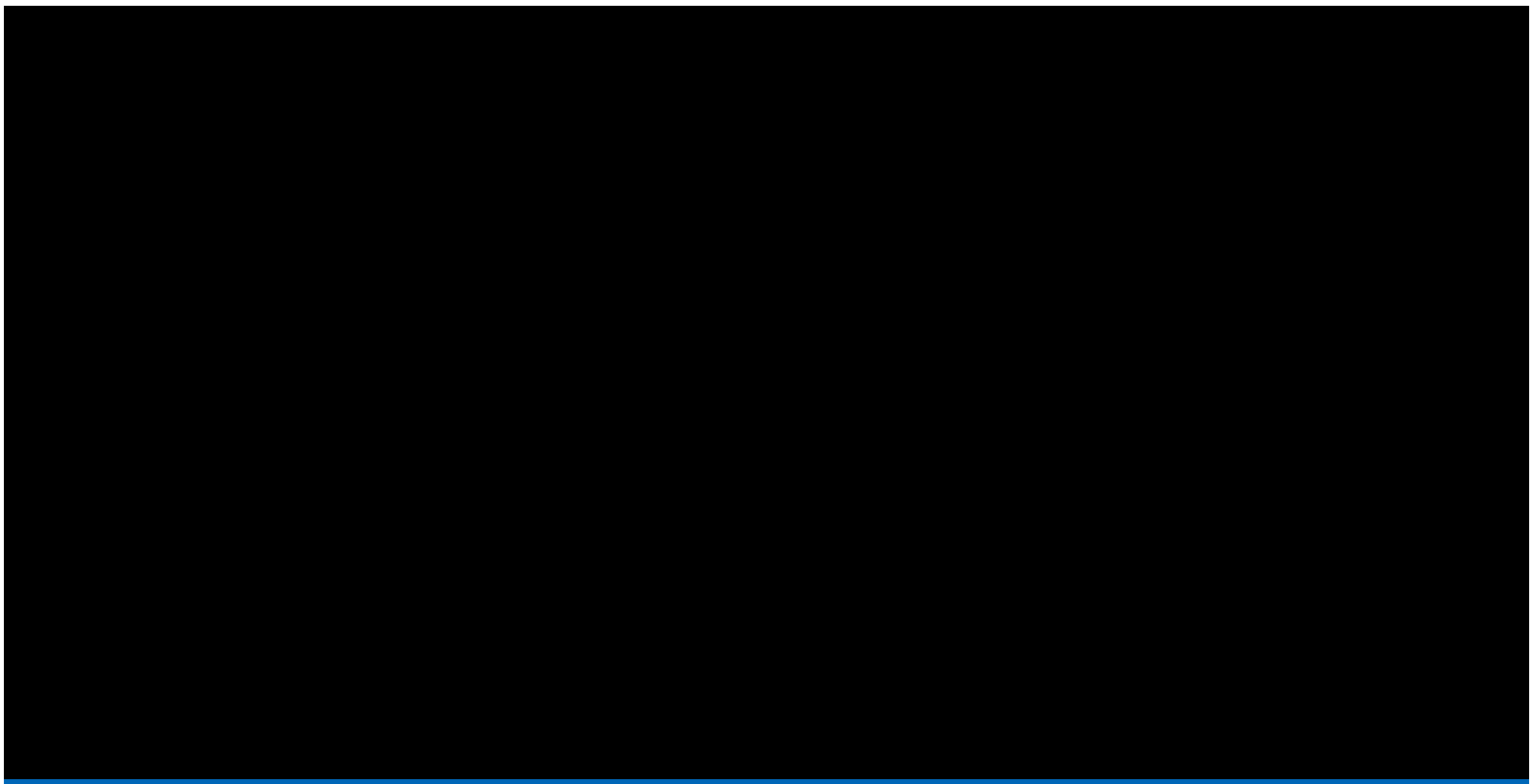


Your data is protected

We rigorously protect your data using encryption and other security best practices.

You can expect privacy by design

We design our products with a core commitment to uphold user privacy.



We stand up for your rights

We fight for stronger privacy laws and protections, and will protect your rights if a government request is made for data.

These principles form the foundation of the Microsoft approach to privacy and will continue to shape the way we build our products and services.

Get more information about how we put those principles into practice.

- We regularly publish the Microsoft Privacy Report to keep you updated about our privacy work.
- We explain how customers can export or delete personal data in our Privacy FAQs.
- We offer in-depth privacy information about our products and services in the Microsoft Privacy Statement.
- We believe that the technology we create should benefit everyone on the planet, and the planet itself. Visit the Microsoft Corporate Social Responsibility for more information.

Privacy dashboard Microsoft Trust Center

Microsoft Privacy Report Government information requests

What's new

Check out the latest articles, blog posts, and news from Microsoft about protecting your privacy at home and at work. (Some content might only be available in English.)

Improve workplace privacy with Microsoft Priva

Microsoft Priva is a new privacy solution designed to help organizations build privacy-resilient workplaces, and empower information workers to make smart data-handling decisions.

Learn more about Microsoft Priva

Microsoft committed to important new milestone for data protection

The European Commission and the U.S. government recently announced the new Trans-Atlantic Data Privacy Framework, an agreement designed to rebuild and strengthen the data protection bridge between the EU and the U.S. Microsoft applauds this important milestone.

Read Julie Brill's blog post about the data agreement

EU Data Boundary for the Microsoft Cloud: A progress report

Read about the important milestone in our journey toward creating the EU Data Boundary for the Microsoft Cloud, and our ongoing commitment to provide customers with robust transparency about our practices and progress toward the implementation of the EU Data Boundary.

Read the EU Data Boundary progress report □

Protecting our data infrastructure through some new approaches to privacy

The question civil society, business, academics and governments should be asking is not if we can use data but rather how we can enable responsible data use to create a better world and protect fundamental human rights. Read about how we're exploring the development of new approaches where needed to enable the responsible use and sharing of data.

Read more about new approaches to privacy □

To learn about managing your privacy settings, see Where can I find privacy settings in Microsoft products?

If you are a resident of the state of California, please see our California Consumer Privacy Act (CCPA) Notice for California Consumers.

We're always working to improve, so if you notice something in our products and services that doesn't work the way you'd expect when it comes to privacy, please let us know.