Microsoft

Microsoft Privacy Statement

Last Updated: August 2018 What's new?

Your privacy is important to us. This privacy statement explains the personal data Microsoft processes, how Microsoft processes it, and for what purposes.

Microsoft offers a wide range of products, including server products used to help operate enterprises worldwide, devices you use in your home, software that students use at school, and services developers use to create and host what's next. References to Microsoft products in this statement include Microsoft services, websites, apps, software, servers, and devices.

Please read the product-specific details in this privacy statement, which provide additional relevant information. This statement applies to the interactions Microsoft has with you and the Microsoft products listed below, as well as other Microsoft products that display this statement.

Personal data we collect

Microsoft collects data from you, through our interactions with you and through our products for a variety of purposes described below, including to operate effectively and provide you with the best experiences with our products. You provide some of this data directly, such as when you create a Microsoft account, administer your organization's licensing account, submit a search query to Bing, register for a Microsoft event, speak a voice command to Cortana, upload a document to OneDrive, purchase an MSDN subscription, sign up for Office 365, or contact us for support. We get some of it by collecting data about your interactions, use, and experience with our products and communications.

We rely on a variety of legal reasons and permissions ("legal bases") to process data, including with your consent, a balancing of legitimate interests, necessity to enter into and perform contracts, and compliance with legal obligations, for a variety of purposes described below.

We also obtain data from third parties. We protect data obtained from third parties according to the practices described in this statement, plus any additional restrictions imposed by the source of the data. These third-party sources vary over time and include:

- Data brokers from which we purchase demographic data to supplement the data we collect.
- Services that make user-generated content from their service available to others, such as local business reviews or public social media posts.
- Communication services, including email providers and social networks, when you give us permission to access your data on such third-party services or networks.

- Service providers that help us determine your device's location.
- Partners with which we offer co-branded services or engage in joint marketing activities.
- Developers who create experiences for Microsoft products, such as Cortana.
- Publicly-available sources, such as open government databases.

If you represent an organization, such as a business or school, that utilizes Enterprise and Developer Products from Microsoft, please see the Enterprise and developer products section of this privacy statement to learn how we process your data.

You have choices when it comes to the technology you use and the data you share. When you are asked to provide personal data, you can decline. Many of our products require some personal data to operate and provide you with a service. If you choose not to provide data necessary to operate and provide you with a product or feature, you cannot use that product or feature. Likewise, where we need to collect personal data by law or to enter into or carry out a contract with you, and you do not provide the data, we will not be able to enter into the contract; or if this relates to an existing product you're using, we may have to suspend or cancel it. We will notify you if this is the case at the time. Where providing the data is optional, and you choose not to share personal data, features like personalization that use the data will not work for you.

The data we collect depends on the context of your interactions with Microsoft and the choices you make (including your privacy settings), the products and features you use, your location, and applicable law.

The data we collect can include the following:

Name and contact data. Your first and last name, email address, postal address, phone number, and other similar contact data.

Credentials. Passwords, password hints, and similar security information used for authentication and account access.

Demographic data. Data about you such as your age, gender, country, and preferred language.

Payment data. Data to process payments, such as your payment instrument number (such as a credit card number) and the security code associated with your payment instrument.

Subscription and licensing data. Information about your subscriptions, licenses, and other entitlements.

Interactions. Data about your use of Microsoft products. In some cases, such as search queries, this is data you provide in order to make use of the products. In other cases, such as error reports, this is data we generate. Other examples of interactions data include:

- **Device and usage data**. Data about your device and the product and features you use, including information about your hardware and software, how our products perform, as well as your settings. For example:
  - **Payment and account history**. Data about the items you purchase and activities

associated with your account.
    - **Browse history**. Data about the webpages you visit.
    - **Device, connectivity, and configuration data**. Data about your device, your device configuration, and nearby networks. For example, data about the operating systems and other software installed on your device, including product keys. In addition, IP address, device identifiers (such as the IMEI number for phones), regional and language settings, and information about WLAN access points near your device.
    - **Error reports and performance data**. Data about the performance of the products and any problems you experience, including error reports. Error reports (sometimes called "crash dumps") can include details of the software or hardware related to an error, contents of files opened when an error occurred, and data about other software on your device.
    - **Troubleshooting and help data**. Data you provide when you contact Microsoft for help, such as the products you use, and other details that help us provide support. For example, contact or authentication data, the content of your chats and other communications with Microsoft, data about the condition of your device, and the products you use related to your help inquiry. When you contact us, such as for customer support, phone conversations or chat sessions with our representatives may be monitored and recorded.
- **Interests and favorites**. Data about your interests and favorites, such as the sports teams you follow, the programming languages you prefer, the stocks you track, or cities you add to track things like weather or traffic. In addition to those you explicitly provide, your interests and favorites can also be inferred or derived from other data we collect.
- **Content consumption data**. Information about media content (e.g., TV, video, music, audio, text books, apps, and games) you access through our products.
- **Searches and commands**. Search queries and commands when you use Microsoft products with search or related productivity functionality.
- **Voice data**. Your voice data, such as the search queries or commands you speak, which may include background sounds.
- **Text, inking, and typing data**. Text, inking, and typing data and related information. For example, when we collect inking data, we collect information about the placement of your inking instrument on your device.
- **Images**. Images and related information, such as picture metadata. For example, we collect the image you provide when you use a Bing image-enabled service.
- **Contacts and relationships**. Data about your contacts and relationships if you use a product to share information with others, manage contacts, communicate with others, or improve your productivity.
- **Social data**. Information about your relationships and interactions between you, other people, and organizations, such as types of engagement (e.g., likes, dislikes, events, etc.) related to people and organizations.
- **Location data**. Data about your device's location, which can be either precise or imprecise. For example, we collect location data using Global Navigation Satellite System (GNSS) (e.g., GPS) and data about nearby cell towers and Wi-Fi hotspots. Location can also be inferred from a device's IP address or data in your account profile that indicates where it is located with less precision, such as at a city or postal code level.

- **Other input**. Other inputs provided when you use our products. For example, data such as the buttons you press on an Xbox wireless controller using Xbox Live, skeletal tracking data when you use Kinect, and other sensor data, like the number of steps you take, when you use devices that have applicable sensors. And, if you use Spend, at your direction, we also collect financial transaction data from your credit card issuer to provide the service.

Content. Content of your files and communications you input, upload, receive, create, and control. For example, if you transmit a file using Skype to another Skype user, we need to collect the content of that file to display it to you and the other user. If you receive an email using Outlook.com, we need to collect the content of that email to deliver it to your inbox, display it to you, enable you to reply to it, and store it for you until you choose to delete it. Other content we collect when providing products to you include:

- Communications, including audio, video, text (typed, inked, dictated, or otherwise), in a message, email, call, meeting request, or chat.
- Photos, images, songs, movies, software, and other media or documents you store, retrieve, or otherwise process with our cloud.

Video or recordings. Recordings of events and activities at Microsoft buildings, retail spaces, and other locations. If you enter Microsoft Store locations or other facilities, or attend a Microsoft event that is recorded, we may process your image and voice data.

Feedback and ratings. Information you provide to us and the content of messages you send to us, such as feedback, survey data, and product reviews you write.

Product-specific sections below describe data collection practices applicable to use of those products.

How we use personal data

Microsoft uses the data we collect to provide you rich, interactive experiences. In particular, we use data to:

- Provide our products, which includes updating, securing, and troubleshooting, as well as providing support. It also includes sharing data, when it is required to provide the service or carry out the transactions you request.
- Improve and develop our products.
- Personalize our products and make recommendations.
- Advertise and market to you, which includes sending promotional communications, targeting advertising, and presenting you relevant offers.

We also use the data to operate our business, which includes analyzing our performance, meeting our legal obligations, developing our workforce, and doing research.

For these purposes, we combine data we collect from different contexts (for example, from your use of two Microsoft products). For example, Cortana uses the favorite sports teams you add to the Microsoft Sports app to provide information relevant to your interests, and Microsoft Store uses

information about the apps and services you use to make personalized app recommendations. However, we have built in technological and procedural safeguards designed to prevent certain data combinations where required by law. For example, where required by law, we store data we collect from you when you are unauthenticated (not signed in) separately from any account information that directly identifies you, such as your name, email address, or phone number.

When we process personal data about you, we do so with your consent and/or as necessary to provide the products you use, operate our business, meet our contractual and legal obligations, protect the security of our systems and our customers, or fulfill other legitimate interests of Microsoft as described in this section and in the Reasons we share personal data section of this privacy statement. When we transfer personal data from the European Economic Area, we do so based on a variety of legal mechanisms, as described in the Where we store and process personal data section of this privacy statement.

More on the purposes of processing:

- **Provide our products.** We use data to operate our products and provide you with rich, interactive experiences. For example, if you use OneDrive, we process the documents you upload to OneDrive to enable you to retrieve, delete, edit, forward, or otherwise process it, at your direction as part of the service. Or, for example, if you enter a search query in the Bing search engine, we use that query to display search results to you. Additionally, as communications are a feature of various products, programs, and activities, we use data to contact you. For example, we may contact you by phone or email or other means to inform you when a subscription is ending or discuss your licensing account. We also communicate with you to secure our products, for example by letting you know when product updates are available.
- **Product improvement.** We use data to continually improve our products, including adding new features or capabilities. For example, we use error reports to improve security features, search queries and clicks in Bing to improve the relevancy of the search results, usage data to determine what new features to prioritize, and voice data to improve speech recognition accuracy.
- **Personalization.** Many products include personalized features, such as recommendations that enhance your productivity and enjoyment. These features use automated processes to tailor your product experiences based on the data we have about you, such as inferences we make about you and your use of the product, activities, interests, and location. For example, depending on your settings, if you stream movies in a browser on your Windows device, you may see a recommendation for an app from the Microsoft Store that streams more efficiently. If you have a Microsoft account, with your permission, we can sync your settings on several devices. Many of our products provide controls to disable personalized features.
- **Product activation.** We use data—such as device and application type, location, and unique device, application, network, and subscription identifiers—to activate products that require activation.
- **Product development.** We use data to develop new products. For example, we use data, often de-identified, to better understand our customers' computing and productivity needs which can shape the development of new products.

- **Customer support.** We use data to troubleshoot and diagnose product problems, repair customers' devices, and provide other customer care and support services.
- **Help secure and troubleshoot.** We use data to help secure and troubleshoot our products. This includes using data to protect the security and safety of our products and customers, detecting malware and malicious activities, troubleshooting performance and compatibility issues to help customers get the most out of their experiences, and notifying customers of updates to our products. This may include using automated systems to detect security and safety issues.
- **Safety.** We use data to protect the safety of our products and our customers. Our security features and products can disrupt the operation of malicious software and notify users if malicious software is found on their devices. For example, some of our products, such as Outlook or OneDrive, systematically scan content in an automated manner to identify suspected spam, viruses, abusive actions, or URLs that have been flagged as fraud, phishing, or malware links; and we reserve the right to block delivery of a communication or remove content if it violates our terms.
- **Updates.** We use data we collect to develop product updates and security patches. For example, we may use information about your device's capabilities, such as available memory, to provide you a software update or security patch. Updates and patches are intended to maximize your experience with our products, help you protect the privacy and security of your data, provide new features, and ensure your device is ready to process such updates.
- **Promotional communications.** We use data we collect to deliver promotional communications. You can sign up for email subscriptions and choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. For information about managing your contact data, email subscriptions, and promotional communications, see the How to access and control your personal data section of this privacy statement.
- **Relevant offers.** Microsoft uses data to provide you with relevant and valuable information regarding our products. We analyze data from a variety of sources to predict the information that will be most interesting and relevant to you and deliver such information to you in a variety of ways. For example, we may predict your interest in gaming and communicate with you about new games you may like.
- **Advertising.** Microsoft does not 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. We use data we collect through our interactions with you, through some of our products, and on third-party web properties, for advertising in our products and on third-party properties. We may use automated processes to help make advertising more relevant to you. For more information about how your data is used for advertising, see the Advertising section of this privacy statement.
- **Transacting commerce.** We use data to carry out your transactions with us. For example, we process payment information to provide customers with product subscriptions and use contact information to deliver goods purchased from the Microsoft Store.
- **Reporting and business operations.** We use data to analyze our operations and perform business intelligence. This enables us to make informed decisions and report on the performance of our business.
- **Protecting rights and property.** We use data to detect and prevent fraud, resolve disputes,

enforce agreements, and protect our property. For example, we use data to confirm the validity of software licenses to reduce piracy. We may use automated processes to detect and prevent activities that violate our rights and the rights of others, such as fraud.

- **Legal compliance.** We process data to comply with law. For example, we use the age of our customers to ensure we meet our obligations to protect children's privacy. We also process contact information and credentials to help customers exercise their data protection rights.
- **Research.** With appropriate technical and organizational measures to safeguard individuals' rights and freedoms, we use data to conduct research, including for public interest and scientific purposes.

Reasons we share personal data

We share your personal data with your consent or as necessary to complete any transaction or provide any product you have requested or authorized. For example, we share your content with third parties when you tell us to do so, such as when you send an email to a friend, share photos and documents on OneDrive, or link accounts with another service. When you provide payment data to make a purchase, we will share payment data with banks and other entities that process payment transactions or provide other financial services, and for fraud prevention and credit risk reduction.

In addition, we share personal data among Microsoft-controlled affiliates and subsidiaries. We also share personal data with vendors or agents working on our behalf for the purposes described in this statement. For example, companies we've hired to provide customer service support or assist in protecting and securing our systems and services may need access to personal data to provide those functions. In such cases, these companies must abide by our data privacy and security requirements and are not allowed to use personal data they receive from us for any other purpose. We may also disclose personal data as part of a corporate transaction such as a merger or sale of assets.

Finally, we will retain, access, transfer, disclose, and preserve personal data, including your content (such as the content of your emails in Outlook.com, or files in private folders on OneDrive), when we have a good faith belief that doing so is necessary to do any of the following:

- Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies.
- Protect our customers, for example, to prevent spam or attempts to defraud users of our products, or to help prevent the loss of life or serious injury of anyone.
- Operate and maintain the security of our products, including to prevent or stop an attack on our computer systems or networks.
- Protect the rights or property of Microsoft, including enforcing the terms governing the use of the services—however, if we receive information indicating that someone is using our services to traffic in stolen intellectual or physical property of Microsoft, we will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement.

For more information about data we disclose in response to requests from law enforcement and other government agencies, please see our Law Enforcement Requests Report.

Please note that some of our products include links to products of third parties whose privacy practices differ from those of Microsoft. If you provide personal data to any of those products, your data is governed by their privacy policies.

How to access and control your personal data

You can access and control your personal data that Microsoft has obtained with tools Microsoft provides to you, which are described below, or by contacting Microsoft. For instance:

- If Microsoft obtained your consent to use your personal data, you can withdraw that consent at any time.
- You can request access to, erasure of, and updates to your personal data.
- If you'd like to port your data elsewhere, you can use tools Microsoft provides to do so, or if none are available, you can contact Microsoft for assistance.

You can also object to or restrict the use of your personal data by Microsoft. For example, you can object at any time to our use of your personal data:

- For direct marketing purposes.
- Where we are performing a task in the public interest or pursuing our legitimate interests or those of a third party.

You may have these rights under applicable laws, including the EU General Data Protection Regulation (GDPR), but we offer them regardless of your location. In some cases, your ability to access or control your personal data will be limited, as required or permitted by applicable law.

If your organization, such as your employer, school, or service provider, provides you with access to and is administering your use of Microsoft products, contact your organization to learn more about how to access and control your personal data.

You can access and control your personal data that Microsoft has obtained, and exercise your data protection rights, using various tools we provide. The tools most useful to you will depend on our interactions with you and your use of our products. Here is a general list of tools we provide to help you control your personal data; specific products may provide additional controls.

- **Microsoft privacy dashboard**. You can control some of the data Microsoft processes through your use of a Microsoft account on the Microsoft privacy dashboard. From here, for example, you can view and clear the browsing, search, and location data associated with your Microsoft account. You can also manage data in your Cortana Notebook and Microsoft Health services.
- **Microsoft account**. If you wish to access, edit, or remove the profile information and payment information in your Microsoft account, change your password, add security information or close your account, you can do so by visiting the Microsoft account website.
- **Volume Licensing Service Center (VLSC)**. If you are a Volume Licensing customer, you can control your contact information and subscription and licensing data in one location by visiting the Volume Licensing Service Center website.

- **Skype**. If you wish to access, edit, or remove profile and payment information in your account for Skype or change your password, sign in to your account.
- **Xbox**. If you use Xbox Live or Xbox.com, you can view or edit your personal data, including billing and account information, privacy settings, and online safety and data sharing preferences by accessing My Xbox on the Xbox console or on the Xbox.com website.
- **Microsoft Store**. You can access your Microsoft Store profile and account information by visiting Microsoft Store and selecting **View account** or **Order history**.
- **Microsoft.com**. You can access and update your profile on microsoft.com by visiting your Microsoft account profile page.
- If you have a **Microsoft Developer Network** (MSDN) public profile, you can access and edit your data by signing in at MSDN forum.

Not all personal data processed by Microsoft can be accessed or controlled via the tools above. If you want to access or control personal data processed by Microsoft that is not available via the tools above or directly through the Microsoft products you use, you can always contact Microsoft at the address in the How to contact us section or by using our web form. We will respond to requests to control your personal data within 30 days.

Your communications preferences

You can choose whether you wish to receive promotional communications from Microsoft by email, SMS, physical mail, and telephone. If you receive promotional email or SMS messages from us and would like to opt out, you can do so by following the directions in that message. You can also make choices about the receipt of promotional email, telephone calls, and postal mail by signing in with your personal Microsoft account, and viewing your communication permissions where you can update contact information, manage Microsoft-wide contact preferences, opt out of email subscriptions, and choose whether to share your contact information with Microsoft partners. If you do not have a personal Microsoft account, you can manage your Microsoft email contact preferences by using this web form. These choices do not apply to mandatory service communications that are part of certain Microsoft products, programs, activities, or to surveys or other informational communications that have their own unsubscribe method.

Your advertising choices

To opt out of receiving interest-based advertising from Microsoft, visit our opt-out page. When you opt out, your preference is stored in a cookie that is specific to the web browser you are using. The opt-out cookie has an expiration date of five years. If you delete the cookies on your device, you need to opt out again.

You can also link your opt-out choice with your personal Microsoft account. It will then apply on any device where you use that account and will continue to apply until someone signs in with a different personal Microsoft account on that device. If you delete the cookies on your device, you will need to sign in again for the settings to apply.

For Microsoft-controlled advertising that appears in apps on Windows, you may use the opt-out linked to your personal Microsoft account, or opt out of interest-based advertising by turning off

the advertising ID in Windows settings.

Because the data used for interest-based advertising is also used for other necessary purposes (including providing our products, analytics, and fraud detection), opting out of interest-based advertising does not stop that data collection. You will continue to get ads, although they may be less relevant to you.

You can opt out of receiving interest-based advertising from third parties we partner with by visiting their sites (see above).

Browser-based controls

When you use a browser, you can control your personal data using certain features. For example:

- **Cookie controls**. You can control the data stored by cookies and withdraw consent to cookies by using the browser-based cookie controls described in the Cookies section of this privacy statement.
- **Tracking protection**. You can control the data third-party sites can collect about you using Tracking Protection in Internet Explorer (versions 9 and up). This feature will block third-party content, including cookies, from any site that is listed in a Tracking Protection List you add.
- **Browser controls for "Do Not Track."** Some browsers have incorporated "Do Not Track" (DNT) features that can send a signal to the websites you visit indicating you do not wish to be tracked. Because there is not yet a common understanding of how to interpret the DNT signal, Microsoft services do not currently respond to browser DNT signals. We continue to work with the online industry to define a common understanding of how to treat DNT signals. In the meantime, you can use the range of other tools we provide to control data collection and use, including the ability to opt out of receiving interest-based advertising from Microsoft as described above.

Cookies and similar technologies

Cookies are small text files placed on your device to store data that can be recalled by a web server in the domain that placed the cookie. This data often consists of a string of numbers and letters that uniquely identifies your computer, but it can contain other information as well. Some cookies are placed by third parties acting on our behalf. We use cookies and similar technologies to store and honor your preferences and settings, enable you to sign-in, provide interest-based advertising, combat fraud, analyze how our products perform, and fulfill other legitimate purposes described below. Microsoft apps use additional identifiers, such as the advertising ID in Windows, for similar purposes, and many of our websites and applications also contain web beacons or other similar technologies, as described below.

Our use of cookies and similar technologies

Microsoft uses cookies and similar technologies for several purposes, depending on the context or product, including:

- **Storing your preferences and settings**. We use cookies to store your preferences and

settings on your device, and to enhance your experiences. For example, if you enter your city or postal code to get local news or weather information on a Microsoft website, depending on your settings, we store that data in a cookie so that you will see the relevant local information when you return to the site. Saving your preferences with cookies, such as your preferred language, prevents you from having to set your preferences repeatedly. If you opt out of interest-based advertising, we store your opt-out preference in a cookie on your device.

- **Sign-in and authentication**. We use cookies to authenticate you. When you sign in to a website using your personal Microsoft account, we store a unique ID number, and the time you signed in, in an encrypted cookie on your device. This cookie allows you to move from page to page within the site without having to sign in again on each page. You can also save your sign-in information so you do not have to sign in each time you return to the site.
- **Security**. We use cookies to process information that helps us secure our products, as well as detect fraud and abuse.
- **Storing information you provide to a website**. We use cookies to remember information you shared. When you provide information to Microsoft, such as when you add products to a shopping cart on Microsoft websites, we store the data in a cookie for the purpose of remembering the information.
- **Social media**. Some of our websites include social media cookies, including those that enable users who are signed in to the social media service to share content via that service.
- **Feedback**. Microsoft uses cookies to enable you to provide feedback on a website.
- **Interest-based advertising**. Microsoft uses cookies to collect data about your online activity and identify your interests so that we can provide advertising that is most relevant to you. You can opt out of receiving interest-based advertising from Microsoft as described in the How to access and control your personal data section of this privacy statement.
- **Showing advertising**. Microsoft uses cookies to record how many visitors have clicked on an advertisement and to record which advertisements you have seen, for example, so you don't see the same one repeatedly.
- **Analytics**. We use first- and third-party cookies and other identifiers to gather usage and performance data. For example, we use cookies to count the number of unique visitors to a web page or service and to develop other statistics about the operations of our products.
- **Performance**. Microsoft uses cookies to understand and improve how our products perform. For example, we use cookies to gather data that helps with load balancing; this helps ensure that our websites remain up and running.

Some of the cookies we commonly use are listed below. This list is not exhaustive, but it is intended to illustrate the primary purposes for which we typically set cookies. If you visit one of our websites, the site will set some or all of the following cookies:

- **MUID, MC1, and MSFPC.** Identifies unique web browsers visiting Microsoft sites. These cookies are used for advertising, site analytics, and other operational purposes.
- **ANON.** Contains the ANID, a unique identifier derived from your Microsoft account, which is used for advertising, personalization, and operational purposes. It is also used to preserve your choice to opt out of interest-based advertising from Microsoft if you have chosen to associate the opt-out with your Microsoft account.

- **CC.** Contains a country code as determined from your IP address.
- **PPAuth, MSPAuth, MSNRPSAuth, KievRPSAuth, WLSSC, MSPProf.** Helps to authenticate you when you sign in with your Microsoft account.
- **MC0.** Detects whether cookies are enabled in the browser.
- **MS0.** Identifies a specific session.
- **NAP.** Contains an encrypted version of your country, postal code, age, gender, language and occupation, if known, based on your Microsoft account profile.
- **MH.** Appears on co-branded sites where Microsoft is partnering with an advertiser. This cookie identifies the advertiser, so the right ad is selected.
- **childinfo, kcdob, kcrelid, kcru, pcfm.** Contains information that Microsoft account uses within its pages in relation to child accounts.
- **MR.** Used to collect information for analytics purposes.
- **x-ms-gateway-slice.** Identifies a gateway for load balancing.
- **TOptOut.** Records your decision not to receive interest-based advertising delivered by Microsoft.

In addition to the cookies Microsoft sets when you visit our websites, third parties can also set cookies when you visit Microsoft sites. For example:

- Companies we hire to provide services on our behalf, such as site analytics, place cookies when you visit our sites. See opt-out links below.
- Companies that deliver content, such as videos or news, or ads on Microsoft sites, place cookies on their own. These companies use the data they process in accordance with their privacy policies, which may enable these companies to collect and combine information about your activities across websites, apps, or online services.

How to control cookies

Most web browsers automatically accept cookies but provide controls that allow you to block or delete them. For example, in Microsoft Edge, you can block or delete cookies by selecting **Settings > Privacy > Cookies**. Please refer to your browser's privacy or help documentation to find Instructions for blocking or deleting cookies in other browsers.

Certain features of Microsoft products depend on cookies. If you choose to block cookies, you cannot sign in or use some of those features, and preferences that are dependent on cookies will be lost. If you choose to delete cookies, any settings and preferences controlled by those cookies, including advertising preferences, are deleted and will need to be recreated.

Additional privacy controls that can impact cookies, including the Tracking Protection feature of Microsoft browsers, are described in the How to access and control your personal data section of this privacy statement.

Our use of web beacons and analytics services

Some Microsoft webpages contain electronic tags known as web beacons that we use to help deliver cookies on our websites, count users who have visited those websites, and deliver co-branded products. We also include web beacons or similar technologies in our electronic

communications to determine whether you open and act on them.

In addition to placing web beacons on our own websites, we sometimes work with other companies to place our web beacons on their websites or in their advertisements. This helps us develop statistics on how often clicking on an advertisement on a Microsoft website results in a purchase or other action on the advertiser's website.

Finally, Microsoft products often contain web beacons or similar technologies from third-party analytics providers, which help us compile aggregated statistics about the effectiveness of our promotional campaigns or other operations. These technologies enable the analytics providers to set or read their own cookies or other identifiers on your device, through which they can collect information about your online activities across applications, websites, or other products. However, we prohibit these analytics providers from using web beacons on our sites to collect or access information that directly identifies you (such as your name or email address). You can opt out of data collection or use by some of these analytics providers by clicking any of the following links: Adjust, AppsFlyer, Clicktale, Flurry Analytics, Google Analytics (requires you to install a browser add-on), Kissmetrics, Mixpanel, Nielsen, Visible Measures, or WebTrends.

Other similar technologies

In addition to standard cookies and web beacons, our products can also use other similar technologies to store and read data files on your computer. This is typically done to maintain your preferences or to improve speed and performance by storing certain files locally. But, like standard cookies, these technologies can also store a unique identifier for your computer, which can then track behavior. These technologies include Local Shared Objects (or "Flash cookies") and Silverlight Application Storage.

Local Shared Objects or "Flash cookies." Websites that use Adobe Flash technologies can use Local Shared Objects or "Flash cookies" to store data on your computer. To learn how to manage or block Flash cookies, go to the Flash Player help page.

Silverlight Application Storage. Websites or applications that use Microsoft Silverlight technology also have the ability to store data by using Silverlight Application Storage. To learn how to manage or block such storage, see the Silverlight section of this privacy statement.

Products provided by your organization—notice to end users

If you use an email address to access Microsoft products and that email address was provided by an organization you are affiliated with, such as an employer or school, that organization can:

- Control and administer your Microsoft product account.
- Access and process your data, including the contents of your communications and files, associated with your Microsoft product accounts.

If you lose access to your work or school account (in event of change of employment, for example), you may lose access to products and the content associated with those products, including those you acquired on your own behalf, if you used your work or school account to sign in to such

products.

Many Microsoft products are intended for use by organizations, such as schools and businesses. Please see the Enterprise and developer products section of this privacy statement. If your organization provides you with access to Microsoft products, your use of the Microsoft products is subject to your organization's policies, if any. You should direct your privacy inquiries, including any requests to exercise your data protection rights, to your organization's administrator. When you use social features in Microsoft products, other users in your network may see some of your activity. To learn more about the social features and other functionality, please review documentation or help content specific to the Microsoft product. Microsoft is not responsible for the privacy or security practices of our customers, which may differ from those set forth in this privacy statement.

Microsoft account

With a Microsoft account, you can sign into Microsoft products, as well as those of select Microsoft partners. Personal data associated with your Microsoft account includes credentials, name and contact data, payment data, device and usage data, your contacts, information about your activities, and your interests and favorites. Signing into your Microsoft account enables personalization, consistent experiences across products and devices, permits you to use cloud data storage, allows you to make payments using payment instruments stored in your Microsoft account, and enables other features. There are three types of Microsoft account:

- When you create your own Microsoft account tied to your personal email address, we refer to that account as a **personal Microsoft account**.
- When you or your organization (such as an employer or your school) create your Microsoft account tied to your email address provided by that organization, we refer to that account as a **work or school account**.
- When you or your service provider (such as a cable or internet service provider) create your Microsoft account tied to your email address with your service provider's domain, we refer to that account as a **third-party account**.

Personal Microsoft accounts. The data associated with your personal Microsoft account, and how that data is used, depends on how you use the account.

- **Creating your Microsoft account**. When you create a personal Microsoft account, you will be asked to provide certain personal data and we will assign a unique ID number to identify your account and associated information. While some products, such as those involving payment, require a real name, you can sign in to and use other Microsoft products without providing your real name. Some data you provide, such as your display name, email address, and phone number, can be used to help others find and connect with you within Microsoft products. For example, people who know your display name, email address, or phone number can use it to search for you on Skype and send you an invite to connect with them. Note that if you use a work or school email address to create a personal Microsoft account, your employer or school may gain access to your data. In some cases, you will need to change the email address to a personal email address in order to continue accessing consumer-oriented products (such as Xbox Live).

- **Signing in to Microsoft account**. When you sign in to your Microsoft account, we create a record of your sign-in, which includes the date and time, information about the product you signed in to, your sign-in name, the unique number assigned to your account, a unique identifier assigned to your device, your IP address, and your operating system and browser version.
- **Signing in to Microsoft products**. Signing in to your account enables improved personalization, provides seamless and consistent experiences across products and devices, permits you to access and use cloud data storage, allows you to make payments using payment instruments stored in your Microsoft account, and enables other enhanced features and settings. When you sign in to your account, you will stay signed in until you sign out. If you add your Microsoft account to a Windows device (version 8 or higher), Windows will automatically sign you in to products that use Microsoft account when you access those products on that device. When you are signed in, some products will display your name or username and your profile photo (if you have added one to your profile) as part of your use of Microsoft products, including in your communications, social interactions, and public posts.
- **Signing in to third-party products**. If you sign in to a third-party product with your Microsoft account, you will share data with the third party in accordance with the third party's privacy policy. The third party will also receive the version number assigned to your account (a new version number is assigned each time you change your sign-in data); and information that describes whether your account has been deactivated. If you share your profile data, the third party can display your name or user name and your profile photo (if you have added one to your profile) when you are signed in to that third-party product. If you chose to make payments to third-party merchants using your Microsoft account, Microsoft will pass information stored in your Microsoft account to the third party or its vendors (e.g., payment processors) as necessary to process your payment and fulfill your order (such as name, credit card number, billing and shipping addresses, and relevant contact information). The third party can use or share the data it receives when you sign in or make a purchase according to its own practices and policies. **You should carefully review the privacy statement for each product you sign in to and each merchant you purchase from to determine how it will use the data it collects.**

Work or school accounts. The data associated with a work or school account, and how it will be used, is generally similar to the use and collection of data associated with a personal Microsoft account.

If your employer or school uses Azure Active Directory (AAD) to manage the account it provides you, you can use your work or school account to sign in to Microsoft products, such as Office 365, and third-party products provided to you by your organization. If required by your organization, you will also be asked to provide a phone number or an alternative email address for additional security verification. And, if allowed by your organization, you may also use your work or school account to sign in to Microsoft or third-party products that you acquire for yourself.

If you sign in to Microsoft products with a work or school account, note:

- The owner of the domain associated with your email address may control and administer your account, and access and process your data, including the contents of your communications

and files, including data stored in products provided to you by your organization, and products you acquire by yourself.
- Your use of the products is subject to your organization's policies, if any. You should consider both your organization's policies and whether you are comfortable enabling your organization to access your data before you choose to use your work or school account to sign in to products you acquire for yourself.
- If you lose access to your work or school account (if you change employers, for example), you may lose access to products, including content associated with those products, you acquired on your own behalf if you used your work or school account to sign in to such products.
- Microsoft is not responsible for the privacy or security practices of your organization, which may differ from those of Microsoft.
- If your organization is administering your use of Microsoft products, please direct your privacy inquiries, including any requests to exercise your data subject rights, to your administrator. See also the Notice to end users section of this privacy statement.

Third-party accounts. The data associated with a third-party Microsoft account, and how it will be used, is generally similar to the use and collection of data associated with a personal Microsoft account. Your service provider has control over your account, including the ability to access or delete your account. **You should carefully review the terms the third party provided you to understand what it can do with your account.**

Other important privacy information

Below you will find additional privacy information, such as how we secure your data, where we process your data, and how long we retain your data. You can find more information on Microsoft and our commitment to protecting your privacy at Microsoft Privacy.

Security of personal data

Microsoft is committed to protecting the security of your personal data. We use a variety of security technologies and procedures to help protect your personal data from unauthorized access, use, or disclosure. For example, we store the personal data you provide on computer systems that have limited access and are in controlled facilities. When we transmit highly confidential data (such as a credit card number or password) over the internet, we protect it through the use of encryption. Microsoft complies with applicable data protection laws, including applicable security breach notification laws.

Where we store and process personal data

Personal data collected by Microsoft may be stored and processed in your region, in the United States, and in any other country where Microsoft or its affiliates, subsidiaries, or service providers operate facilities. Microsoft maintains major data centers in Australia, Austria, Brazil, Canada, Chile, Finland, France, Germany, Hong Kong, India, Ireland, Japan, Korea, Luxembourg, Malaysia, the Netherlands, Singapore, South Africa, the United Kingdom, and the United States. Typically, the primary storage location is in the customer's

region or in the United States, often with a backup to a data center in another region. The storage location(s) are chosen in order to operate efficiently, to improve performance, and to create redundancies in order to protect the data in the event of an outage or other problem. We take steps to ensure that the data we collect under this privacy statement is processed according to the provisions of this statement and the requirements of applicable law wherever the data is located.

We transfer personal data from the European Economic Area and Switzerland to other countries, some of which have not yet been determined by the European Commission to have an adequate level of data protection. For example, their laws may not guarantee you the same rights, or there may not be a privacy supervisory authority there that is capable of addressing your complaints. When we engage in such transfers, we use a variety of legal mechanisms, including contracts, to help ensure your rights and protections travel with your data. To learn more about the European Commission's decisions on the adequacy of the protection of personal data in the countries where Microsoft processes personal data, see this article on the European Commission website.

Microsoft Corporation complies with the EU-U.S. Privacy Shield Framework and Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union and Switzerland to the United States. Microsoft Corporation has certified to the Department of Commerce that it adheres to the Privacy Shield Principles. If third-party agents process personal data on our behalf in a manner inconsistent with the principles of either Privacy Shield framework, we remain liable unless we prove we are not responsible for the event giving rise to the damage. The controlled U.S. subsidiaries of Microsoft Corporation, as identified in our self-certification submission, also adhere to the Privacy Shield Principles—for more info, see the list of Microsoft U.S. entities or subsidiaries adhering to the Privacy Shield Principles.

If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, visit the Privacy Shield website.

If you have a question or complaint related to participation by Microsoft in the EU-U.S. or Swiss-U.S. Privacy Shield, we encourage you to contact us via our web form. For any complaints related to the Privacy Shield frameworks that Microsoft cannot resolve directly, we have chosen to cooperate with the relevant Data Protection Authority, or a panel established by the European data protection authorities for resolving disputes. Please contact us if you'd like us to direct you to your data protection authority contacts. As further explained in the Privacy Shield Principles, binding arbitration is available to address residual complaints not resolved by other means. Microsoft is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

Our retention of personal data

Microsoft retains personal data for as long as necessary to provide the products and fulfill

the transactions you have requested, or for other legitimate purposes such as complying with our legal obligations, resolving disputes, and enforcing our agreements. Because these needs can vary for different data types, the context of our interactions with you or your use of products, actual retention periods can vary significantly.

Other criteria used to determine the retention periods include:

- **Do customers provide, create, or maintain the data with the expectation we will retain it until they affirmatively remove it?** Examples include a document you store in OneDrive, or an email message you keep in your Outlook.com inbox. In such cases, we would aim to maintain the data until you actively delete it, such as by moving an email from your Outlook.com inbox to the Deleted Items folder, and then emptying that folder (when your Deleted Items folder is emptied, those emptied items remain in our system for up to 30 days before final deletion). (Note that there may be other reasons why the data has to be deleted sooner, for example if you exceed limits on how much data can be stored in your account.)
- **Is there an automated control, such as in the Microsoft privacy dashboard, that enables the customer to access and delete the personal data at any time?** If there is not, a shortened data retention time will generally be adopted.
- **Is the personal data of a sensitive type?** If so, a shortened retention time would generally be adopted.
- **Has Microsoft adopted and announced a specific retention period for a certain data type?** For example, for Bing search queries, we de-identify stored queries by removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers after 18 months.
- **Has the user provided consent for a longer retention period?** If so, we will retain data in accordance with your consent.
- **Is Microsoft subject to a legal, contractual, or similar obligation to retain or delete the data?** Examples can include mandatory data retention laws in the applicable jurisdiction, government orders to preserve data relevant to an investigation, or data retained for the purposes of litigation. Conversely, if we are required by law to remove unlawful content, we will do so.

Advertising

Advertising allows us to provide, support, and improve some of our products. Microsoft does not 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. We use other data, detailed below, for advertising in our products and on third-party properties. For example:

- Microsoft may use data we collect to select and deliver some of the ads you see on Microsoft web properties, such as Microsoft.com, MSN, and Bing.
- When the advertising ID is enabled in Windows 10 as part of your privacy settings, third parties can access and use the advertising ID (much the same way that websites can access and use a unique identifier stored in a cookie) to select and deliver ads in

such apps.
- We may share data we collect with third parties, such as Oath, AppNexus, or Facebook (see below), so that the ads you see in our products, their products, or other sites and apps serviced by these partners are more relevant and valuable to you.
- Advertisers may choose to place our web beacons on their sites, or use similar technologies, in order to allow Microsoft to collect information on their sites such as activities, purchases, and visits; we use this data on behalf of our advertising customers to provide ads.

The ads that you see may be selected based on data we process about you, such as your interests and favorites, your location, your transactions, how you use our products, your search queries, or the content you view. For example, if you view content on MSN about automobiles, we may show advertisements about cars; if you search “pizza places in Seattle” on Bing, you may see advertisements in your search results for restaurants in Seattle.

The ads that you see may also be selected based on other information learned about you over time using demographic data, location data, search queries, interests and favorites, usage data from our products and sites, as well as the sites and apps of our advertisers and partners. We refer to these ads as "interest-based advertising" in this statement. For example, if you view gaming content on xbox.com, you may see offers for games on MSN. To provide interest-based advertising, we combine cookies placed on your device using information that we collect (such as IP address) when your browser interacts with our websites. If you opt out of receiving interest-based advertising, data associated with these cookies will not be used.

Further details regarding our advertising-related uses of data include:

- **Advertising industry best practices and commitments**. Microsoft is a member of the Network Advertising Initiative (NAI) and adheres to the NAI Code of Conduct. We also adhere to the following self-regulatory programs:
  - In the US: Digital Advertising Alliance (DAA)
  - In Europe: European Interactive Digital Advertising Alliance (EDAA)
  - In Canada: Ad Choices: Digital Advertising Alliance of Canada (DAAC) / Choix de Pub: l'Alliance de la publicité numérique du Canada (DAAC)
- **Health-related ad targeting**. In the United States, we provide interest-based advertising based on a limited number of standard, non-sensitive health-related interest categories, including allergies, arthritis, cholesterol, cold and flu, diabetes, gastrointestinal health, headache / migraine, healthy eating, healthy heart, men’s health, oral health, osteoporosis, skin health, sleep, and vision / eye care. We will also target ads based on custom, non-sensitive health-related interest categories as requested by advertisers.
- **Children and advertising**. We do not deliver interest-based advertising to children whose birthdate in their Microsoft account identifies them as under 16 years of age.
- **Data retention**. For interest-based advertising, we retain data for no more than 13 months, unless we obtain your consent to retain the data longer.
- **Data sharing**. In some cases, we share with advertisers reports about the data we

have collected on their sites or ads.

Data collected by other advertising companies. Advertisers sometimes include their own web beacons (or those of their other advertising partners) within their advertisements that we display, enabling them to set and read their own cookie. Additionally, Microsoft partners with third-party ad companies to help provide some of our advertising services, and we also allow other third-party ad companies to display advertisements on our sites. These third parties may place cookies on your computer and collect data about your online activities across websites or online services. These companies currently include, but are not limited to: A9, AppNexus, Criteo, Facebook, MediaMath, nugg.adAG, Oath, Rocket Fuel, and Yahoo!. Select any of the preceding links to find more information on each company's practices, including the choices it offers. Many of these companies are also members of the NAI or DAA, which each provide a simple way to opt out of ad targeting from participating companies.

Collection of data from children

When a Microsoft product collects age, and there is an age in your jurisdiction under which parental consent or authorization is required to use the product, the product will either block users under that age or will ask them to provide consent or authorization from a parent or guardian before they can use it. We will not knowingly ask children under that age to provide more data than is necessary to provide for the product.

Once parental consent or authorization is granted, the child's account is treated much like any other account. The child can access communication services, like Outlook and Skype, and can freely communicate and share data with other users of all ages.

Parents can change or revoke the consent choices previously made, and review, edit, or request the deletion of the personal data of children for whom they provided consent or authorization. For example, parents can access their personal Microsoft account and select **Permissions**. For users of Minecraft for PC/Java and other Mojang games, parents can visit the Mojang Account page.

Preview or free-of-charge releases

Microsoft offers preview, insider, beta or other free-of-charge products and features ("previews") to enable you to evaluate them while providing Microsoft with data about your use of the product, including feedback and device and usage data. As a result, previews can automatically collect additional data, provide fewer controls, and otherwise employ different privacy and security measures than those typically present in our products. If you participate in previews, we may contact you about your feedback or your interest in continuing to use the product after general release.

Changes to this privacy statement

We update this privacy statement when necessary to provide greater transparency or in response to:

- Feedback from customer, regulators, industry, or other stakeholders.
- Changes in our products.
- Changes in our data processing activities or policies.

When we post changes to this statement, we will revise the "last updated" date at the top of the statement and describe the changes on the Change history page. If there are material changes to the statement, such as a change to the purposes of processing of personal data that is not consistent with the purpose for which it was originally collected, we will notify you either by prominently posting a notice of such changes before they take effect or by directly sending you a notification. We encourage you to periodically review this privacy statement to learn how Microsoft is protecting your information.

How to contact us

If you have a privacy concern, complaint, or question for the Microsoft Chief Privacy Officer or Data Protection Officer, please contact us by using our web form. We will respond to questions or concerns within 30 days. You can also raise a concern or lodge a complaint with a data protection authority or other official with jurisdiction.

Unless otherwise stated, Microsoft Corporation and, for those in the European Economic Area and Switzerland, Microsoft Ireland Operations Limited are data controllers for personal data we collect through the products subject to this statement. Our addresses are:

- Microsoft Privacy, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, USA. Telephone: +1 (425) 882 8080.
- Microsoft Ireland Operations Limited, Attn: Data Protection Officer, One Microsoft Place, South County Business Park, Leopardstown, Dublin 18, Ireland. Telephone: +353 (0) 1 295 3826.

Skype Communications S.à r.l. 23-29 Rives de Clausen L-2165 Luxembourg, Luxembourg, is a data controller for Skype. To contact us in relation to Skype software or products, please visit the Skype Help page to submit a support request to the Skype customer support team.

To find the Microsoft subsidiary in your country or region, see the list of Microsoft office locations around the world.

Where French law applies, you can also send us specific instructions regarding the use of your personal data after your death, by using our web form.

If you have a technical or support question, please visit Microsoft Support to learn more about Microsoft Support offerings. If you have a personal Microsoft account password question, please visit Microsoft account support.

Enterprise and developer products

Enterprise and Developer Products are Microsoft products and related software offered to and designed primarily for use by organizations and developers. They include:

- Cloud services, referred to as Online Services in the Microsoft Online Services Terms (OST), such as Office 365, Microsoft Azure, Microsoft Dynamics365, and Microsoft Intune, for which an organization (our customer) contracts with Microsoft for the services ("Enterprise Online Services").
- Server and developer products, such as Windows Server, SQL Server, Visual Studio, and System Center ("Enterprise and Developer Software").
- Appliances and hardware used for storage infrastructure, such as StorSimple ("Enterprise Appliances").
- Developer services such as Bot Framework, Cortana Skills Kit, and Botlet Store.
- Professional services referred to in the OST that are available with Enterprise Online Services, such as onboarding services, data migration services, data science services, or services to supplement existing features in the Enterprise Online Services.

In the event of a conflict between this Microsoft privacy statement and the terms of any agreement(s) between a customer and Microsoft for Enterprise and Developer Products, the terms of those agreement(s) will control.

You can also learn more about our Enterprise and Developer Products' features and settings, including choices that impact your privacy or your end users' privacy, in product documentation.

If any of the terms below are not defined in this Privacy Statement or the OST, they have the definitions below.

General. When a customer tries, purchases, uses, or subscribes to Enterprise and Developer Products, or obtains support for or professional services with such products, Microsoft collects data to provide the service (including uses compatible with providing the service), provide the best experiences with our products, operate our business, and communicate with the customer. For example:

- When a customer engages with a Microsoft sales representative, we collect the customer's name and contact data, along with information about the customer's organization, to support that engagement.
- When a customer interacts with a Microsoft support professional, we collect device and usage data or error reports to diagnose and resolve problems.
- When a customer pays for products, we collect contact and payment data to process the payment.
- When Microsoft sends communications to a customer, we use data to personalize the content of the communication.
- When a customer engages with Microsoft for professional services, we collect the name and contact data of the customer's designated point of contact and use information provided by the customer to perform the services that the customer has requested.

The Enterprise and Developer Products enable you to purchase, subscribe to, or use other products and online services from Microsoft or third parties with different privacy practices, and those other products and online services are governed by their respective privacy statements and policies.

Enterprise online services

To provide the Enterprise Online Services, Microsoft collects Customer Data, Administrator Data, Payment Data, and Support Data.

We use Customer Data, Support Data, and Personal Data as described in the OST and the Microsoft Trust Center. Customer is the controller of Personal Data and Microsoft is the processor of such data, except when (a) Customer acts as a processor of Personal Data, in which case Microsoft is a subprocessor or (b) stated otherwise in the OST.

Administrator Data is the information provided to Microsoft during sign-up, purchase, or administration of Enterprise Online Services. We use Administrator Data to provide the Enterprise Online Services, complete transactions, service the account, detect and prevent fraud, and comply with our legal obligations. Administrator Data includes the name, address, phone number, and email address you provide, as well as aggregated usage data related to your account, such as the controls you select. Administrator Data also includes contact information of your colleagues and friends if you agree to provide it to Microsoft for the limited purpose of sending them an invitation to use the Enterprise Online Services; we contact those individuals with communications that include information about you, such as your name and profile photo.

As needed, we use Administrator Data to contact you to provide information about your account, subscriptions, billing, and updates to the Enterprise Online Services, including information about new features, security, or other technical issues. We also contact you regarding third-party inquiries we receive regarding use of the Enterprise Online Services, as described in your agreement. You cannot unsubscribe from these non-promotional communications. We may also contact you regarding information and offers about other products and services, or share your contact information with Microsoft's partners. When such a partner has specific services or solutions to meet your needs, or to optimize your use of the Enterprise Online Services, we may share limited, aggregated information about your organization’s account with the partner. Microsoft will not share your confidential information or contact information with the authorized partner unless we have sufficient rights to do so. You can manage your contact preferences or update your information in your account profile.

We use payment data to complete transactions, as well as to detect and prevent fraud.

Some Enterprise Online Services require, or are enhanced by, the installation of local software (e.g., agents, device management applications) on a device. At your direction, the local software may transmit (i) data, which can include Customer Data, from a device or appliance to or from the Enterprise Online Services; or (ii) logs or error reports to Microsoft for troubleshooting purposes. The Enterprise Online Services, including local software,

collect device and usage data that is transmitted to Microsoft and analyzed to improve the quality, security, and integrity of our products.

Bing Search Services, as defined in the OST, use data such as search queries as described in the Bing section of this privacy statement.

Enterprise and developer software and enterprise appliances

Enterprise and developer software and enterprise appliances collect data to operate effectively and provide you the best experiences. The data we collect depends on the features you use, as well as your configuration and settings, but it is generally limited to device and usage data. Customers have choices about the data they provide. Here are examples of the data we collect:

- During installation or when you upgrade an enterprise and developer software, we may collect device and usage data to learn whether you experience any difficulties.
- When you use enterprise software or enterprise appliances, we may collect device and usage data to learn about your operating environment to improve security features.
- When you experience a crash using enterprise software or enterprise appliances, you may choose to send Microsoft an error report to help us diagnose the problem and deliver customer support.

Microsoft uses the data we collect from enterprise and developer software and enterprise appliances to provide and improve our products, to deliver customer support, to activate the product, to communicate with you, and to operate our business.

Microsoft SQL Server is a relational database management platform and includes products that can be installed separately (such as SQL Server Management Studio). For detailed information about what data we collect, how we use it, and how to manage your privacy options, visit the SQL Server privacy page. If you work in an organization, your administrator can set certain telemetry settings in SQL Server via Group Policy.

Productivity and communications products

Productivity and communications products are applications, software, and services you can use to create, store, and share documents, as well as communicate with others.

Office

Office is a collection of productivity applications including Word, Excel, PowerPoint, OneNote, and Outlook, among others. For more details about Outlook, see the Outlook section of this privacy statement. Various Office applications enable you to use content and functionality from other Microsoft products, such as Bing, and third-party connected products. If you work in an organization, your administrator can turn off or disable these connected services. You can access privacy settings in Office 2016 by selecting **File** > **Options** > **Trust Center** > **Trust Center Settings** > **Privacy Options**. For detailed

information, see View my options and settings in the Microsoft Outlook Trust Center.

Office Roaming Service. The Office Roaming Service helps keep your Office settings up to date across your devices running Office. When you sign in to Office with your Microsoft account or an account issued by your organization, the Office Roaming Service is turned on and syncs some of your customized Office settings to Microsoft servers (such as a list of most recently used documents and the last location viewed within a document). When you sign in to Office on another device with the same account, the Office Roaming Service downloads your settings from Microsoft servers and applies them to the additional device. The Office Roaming Service also applies some of your customized Office settings when you sign in to Office.com. When you sign out of Office, the Office Roaming Service removes your Office settings from your device. Any changes you made to your customized Office settings are sent to Microsoft servers.

Microsoft Updates. Office uses the Microsoft Update service to provide you with security and other important updates. See the Update Services section of this privacy statement for more information.

Online help, templates, and fonts. Office uses other Microsoft or third-party services to give you the latest online content when you are connected to the internet, such as Help articles, templates, and fonts. The online fonts feature can be disabled by an administrative group policy setting, while other online content can be turned off by using privacy settings as described above. Online templates are made available to you when you start a new document. When you use the Help feature in Office applications, Office sends your search query to Office.com to provide you with online help articles. If online services are disabled, clicking on Help will take you to support.office.com in your default browser.

Click-to-Run Update Service. The Click-to-Run Update Service allows you to install certain Microsoft Office products over the internet, so you can start using them before they are completely downloaded. The Click-to-Run Update Service also automatically detects online updates to Click-to-Run-enabled products on your device and downloads and installs them automatically. You can turn the service off by using privacy settings.

Recommendation services. Some Office services send customer data to Microsoft to provide the user with recommendations. For example, Editor helps the user improve writing in Word. When a word is misspelled, that word and a few words around it are sent to Microsoft and analyzed to suggest the correct spelling. Editor will also check for poor grammar as the user is drafting. In PowerPoint, a user can send content to the Designer service to get professionally designed layout suggestions. This data may also be used to improve Microsoft products.

Search services. Office-supported search services allow you to request information from Microsoft or third-party services from within an Office application. For example, in Word, you can highlight a word or phrase and retrieve relevant information from Bing search. When you search using a particular word or phrase, Office sends that text to the service in encrypted form. To provide you with contextually relevant search results, Office will send

your requested word or phrase and some surrounding content from your document. In Excel, you can use Insights to send categories of data to Microsoft to receive recommendations for other sets of similar data that might interest you, but the actual content from your workbook isn't sent to Microsoft. In addition, Office will send data about the Office software and system you're using, including the version, operating system, locale, and language setting. If required by a third-party content provider, it will also send authorization data indicating you have the right to download the relevant content. Frequently, the information you receive includes a link to additional information from the content provider's website. If you click the link, the content provider may place a cookie on your device.

Translation service. Some Office applications allow you to translate text using machine translation. You may send text from your document, which is encrypted by the Office application before being sent, to the Microsoft Translator service. In addition to the specific text you want to translate, Office may send some surrounding text from your document to provide a more relevant translation. You can also choose to send your entire document for translation. To learn more, see the Microsoft Translator section of this privacy statement.

OneDrive

OneDrive lets you store and access your files on virtually any device. You can also share and collaborate on your files with others. Some versions of the OneDrive application enable you to access both your personal OneDrive by signing in with your personal Microsoft account and your OneDrive for Business by signing in with your work or school Microsoft account as part of your organization's use of Office 365.

When you use OneDrive, we collect data about your usage of the service, as well as the content you store, to provide, improve, and protect the services. Examples include indexing the contents of your OneDrive documents so that you can search for them later and using location information to enable you to search for photos based on where the photo was taken. We also collect device information so we can deliver personalized experiences, such as enabling you to sync content across devices and roam customized settings.

When you store content in OneDrive, that content will inherit the sharing permissions of the folder in which you store it. For example, if you decide to store content in the public folder, the content will be public and available to anyone on the internet who can find the folder. If you store content in a private folder, the content will be private.

When you share content to a social network like Facebook from a device that you have synced with your OneDrive account, your content is either uploaded to that social network, or a link to that content is posted to that social network. Doing this makes the content accessible to anyone on that social network. To delete the content, you need to delete it from the social network (if it was uploaded there, rather than a link to it) and from OneDrive.

When you share your OneDrive content with your friends via a link, an email with the link is

sent to those friends. The link contains an authorization code that allows anyone with the link to access your content. If one of your friends sends the link to other people, they will also be able to access your content, even if you did not choose to share the content with them. To revoke permissions for your content on OneDrive, sign in to your account and then select the specific content to manage the permission levels. Revoking permissions for a link effectively deactivates the link. No one will be able to use the link to access the content unless you decide to share the link again.

Files managed with OneDrive for Business are stored separately from files stored with your personal OneDrive. OneDrive for Business collects and transmits personal data for authentication, such as your email address and password, which will be transmitted to Microsoft and/or to the provider of your Office 365 service.

Outlook

Outlook products are designed to improve your productivity through improved communications and include Outlook.com, Outlook applications, and related services.

Outlook.com. Outlook.com is the primary consumer email service from Microsoft and includes email accounts with addresses that end in outlook.com, live.com, hotmail.com, and msn.com. Outlook.com provides features that let you connect with your friends on social networks. You will need to create a Microsoft account to use Outlook.com.

When you delete an email or item from a mailbox in Outlook.com, the item generally goes into your Deleted Items folder where it remains for approximately 7 days unless you move it back to your inbox, you empty the folder, or the service empties the folder automatically, whichever comes first. When the Deleted Items folder is emptied, those emptied items remain in our system for up to 30 days before final deletion, unless we are legally required to retain the data for longer.

Outlook applications. Outlook client applications are software you install on your device that permits you to manage email, calendar items, files, contacts, and other data from email, file storage, and other services, like Exchange Online or Outlook.com, or servers, like Microsoft Exchange. You can use multiple accounts from different providers, including third-party providers, with Outlook applications.

To add an account, you must provide permission for Outlook to access data from the email or file storage services.

When you add an account to Outlook, your mail, calendar items, files, contacts, settings and other data from that account will automatically sync to your device. If you are using the mobile Outlook application, that data will also sync to Microsoft servers to enable additional features such as faster search, personalized filtering of less important mail, and an ability to add email attachments from linked file storage providers without leaving the Outlook application. If you are using the desktop Outlook application, you can choose whether to allow the data to sync to our servers. At any time, you can remove an account or

make changes to the data that is synced from your account.

If you add an account provided by an organization (such as your employer or school), the owner of the organizational domain can implement policies and controls (for example, requiring multi-factor authentication or the ability to remotely wipe data from your device) that can affect your use of Outlook.

To learn more about the data the Outlook applications collect and process, please see the Office section of this privacy statement.

Skype

Skype lets you send and receive voice, video, and instant message communications. This section applies to the consumer version of Skype; if you are using Skype for Business, see the Enterprise and developer products section of this privacy statement.

As part of providing these features, Microsoft collects usage data about your communications that includes the time and date of the communication and the numbers or user names that are part of the communication.

Skype profile. To enable other people to find you on Skype (or products that interact with Skype, such as Skype for Business), depending on your profile settings, your Skype profile is included in the Skype public search directory and may be recommended to other users. Your profile includes your user name, avatar, and any other data you choose to add to your profile or display to others.

Skype Contacts. If you use a Microsoft service, such as Outlook.com, to manage contacts, Skype will automatically add the people you know to your Skype contact list until you tell us to stop. With your permission, Skype will also check your device or other address books from time to time to automatically add your friends as Skype contacts. You can block users if you don't want to receive their communications.

Partner companies. To make Skype available to more people, we partner with other companies to allow Skype to be offered via those companies' services. If you use Skype through a company other than Microsoft, that company's privacy policy governs how it handles your data. To comply with applicable law or respond to valid legal process, or to help our partner company or local operator comply or respond, we may access, transfer, disclose, and preserve your data. That data could include, for example, your private content, such as the content of your instant messages, stored video messages, voicemails, or file transfers.

Skype Manager. Skype Manager lets you manage a group's (such as your family's) Skype usage from one central place. When you set up a group, you will be the Skype Manager Administrator and can see the patterns of usage, including detailed information, like traffic data and details of purchases, of other members of the group who have consented to such access. If you add information like your name, other people in the group will be able to see

it. Members of the group can withdraw consent for Skype Manager by visiting their Skype account page.

Push notifications. To let you know of incoming calls, chats, and other messages, Skype apps use the notification service on your device. For many devices, these services are provided by another company. To tell you who is calling, for example, or to give you the first few words of the new chat, Skype has to tell the notification service so that they can provide the notification to you. The company providing the notification service on your device will use this information in accordance with their own terms and privacy policy. Microsoft is not responsible for the data collected by the company providing the notification service. If you don't want to use the notification services for incoming Skype calls and messages, turn it off in the settings found in the Skype application or your device.

Skype advertising. Some Skype software includes interest-based advertising, so that you're more likely to see ads you'll like. In some versions of the software, you can opt out of interest-based advertising in the privacy options or account settings menu. If you sign in to Skype with a Microsoft account, you can opt out of interest-based advertising on the Microsoft privacy dashboard. If you opt out, you'll still see ads displayed in the Skype software based on your country of residence, language preference, and IP address location, but other data is not used for ad targeting.

Translation features. To help you communicate with people in different languages, some Skype apps offer audio and/or text translation features. When you use translation features, your voice and text data are used to provide and improve Microsoft speech recognition and translation services.

Recording features. Some versions of Skype have a recording feature that allows you to capture and share all or part of your audio / video call. The recording will be stored and shared as part of your conversation history with the person or group with whom the call occurred. **You should understand your legal responsibilities before recording any communication. This includes whether you need to get consent from all parties to the communication in advance**. Microsoft is not responsible for how you use your recordings or the recording features.

Skype bots. Bots are programs offered by Microsoft or third parties that can do many useful things like search for news, play games, and more. Depending on their capabilities, bots may have access to your display name, Skype ID, country, region, language, and any messages, audio, video, or content that you share with the bot. Please review the bot profile and its privacy statement before engaging in a one-to-one or group conversation with a bot. You can delete a bot that you no longer wish to engage with. Prior to adding a bot to a group, please ensure that your group participants have consented to their information being shared with the bot.

Cortana in Skype. Subject to availability, you can use Cortana in Skype to help manage your time and tasks, find information, and get things done using Microsoft and third-party services. Cortana works best when you give her permission to use data, such as your

location and IM conversations from Skype to personalize experiences across Microsoft products that offer Cortana functionality. If you choose not to give permission, Cortana may still provide you with non-personalized suggestions and responses within Skype.

LinkedIn

To learn about the data LinkedIn collects and how it is used and shared, please see LinkedIn's Privacy Policy.

Search and artificial intelligence

Search and artificial intelligence products connect you with information and intelligently sense, process, and act on information—learning and adapting over time.

Bing

Bing services include search and mapping services, as well as the Bing Toolbar and Bing Desktop apps. Bing services collect and process data in many forms, including text that has been inked or typed, speech data, and images. Bing services are also included within other Microsoft services, such as MSN Apps, Office, Cortana, and certain features in Windows (which we refer to as Bing-powered experiences).

When you conduct a search, or use a feature of a Bing-powered experience that involves conducting a search or entering a command on your behalf, Microsoft will collect the searches or commands you provide (which may be in the form of text, voice data, or an image), along with your IP address, location, the unique identifiers contained in our cookies or similar technologies, the time and date of your search, and your browser configuration. For example, if you use Bing voice-enabled services, your voice input and performance data associated with the speech functionality will be sent to Microsoft. And, if you use Bing image-enabled services, the image you provide will be sent to Microsoft. When you use Bing-powered experiences, such as Ask Cortana or Bing Lookup to search a particular word or phrase within a webpage or document, that word or phrase is sent to Bing along with some surrounding content in order to provide contextually relevant search results.

Search suggestions. For the search suggestions feature, the characters that you type into a Bing-powered experience to conduct a search will be sent to Microsoft. This allows us to provide you with suggestions as you type your searches. To turn this feature on or off, while using Bing Search, go to Bing Settings. Search Suggestions cannot be turned off in Cortana. On Windows, you can always hide Cortana and the search box so as not to use the feature.

Bing experience improvement program for Bing Desktop and Bing Toolbar. If you are using Bing Desktop or Bing Toolbar and choose to participate in the Bing Experience Improvement Program, we also collect additional data about how you use these specific Bing apps, such as the addresses of the websites you visit, to help improve search ranking and relevance. To help protect your privacy, we do not use the data collected through the

Bing Experience Improvement Program to identify or contact you or target advertising to you. You can turn off the Bing Experience Improvement Program at any time in the Bing Desktop or Bing Toolbar settings. Finally, we delete the information collected through the Bing Experience Improvement Program after 18 months.

Retention and de-identification. We de-identify stored search queries by removing the entirety of the IP address after 6 months, and cookie IDs and other cross-session identifiers after 18 months.

Personalization through Microsoft account. Some Bing services provide you with an enhanced experience when you sign in with your personal Microsoft account, for example, syncing your search history across devices. You can use these personalization features to customize your interests, favorites, and settings, and to connect your account with third-party services. Visit Bing Settings to manage your personalization settings, or the Microsoft privacy dashboard to manage your data.

Managing search history. When you're signed-in to a personal Microsoft account, you can erase your search history on the Microsoft privacy dashboard. The Search History service from Bing, located in Bing Settings, provides another method of revisiting the search terms you've entered and results you've clicked when using Bing search through your browser. You may clear your search history on a device through this service. Clearing your history prevents that history from being displayed on the Search History site, but does not delete information from our search logs, which are retained and de-identified as described above or as you have instructed through the privacy dashboard.

Third-party services that use Bing. You may access Bing-powered experiences when using third-party services, such as those from Yahoo!. In order to provide these services, Bing receives data from these and other partners, including your search query and related data (such as date, time, IP address, and a unique identifier). This data will be sent to Microsoft to provide the search service. Microsoft will use this data as described in this statement or as further limited by our contractual obligations with our partners. You should refer to the privacy policies of the third-party services for any questions about how they collect and use data.

Search query passed in referral URL. When you select a search result or advertisement from a Bing search results page and go to the destination website, the destination website will receive the standard data your browser sends to every web site you visit—such as your IP address, browser type and language, and the URL of the site you came from (in this case, the Bing search results page). Because the URL of the Bing search results page contains the text of the search query you entered (which could include names, addresses, or other identifying information), the destination website will be able to determine the search term you entered.

If your browser is enabled to allow pages to pre-load in the background for faster performance, when your browser loads a page in the background, it will have the same effect as if you visited that page, including sending the Bing search results page URL

(containing your search query) and downloading any cookies or similar technologies that page sets.

Sharing data from Bing and Bing-powered experiences with third parties. We share some de-identified data (data where the identity of a specific person is not known) from Bing and Bing-powered experiences with selected third parties. Before we do so, we run the data through a process designed to remove certain sensitive data that users may have included in the search terms themselves (such as social security numbers or credit card numbers). Additionally, we require these third parties to keep the data secure and to not use the data for purposes other than for which it is provided.

Cortana

Cortana is your intelligent assistant that provides smart features and personalized experiences across a variety of devices, apps, and services. As described below, the data we collect when you use Cortana depends on the choices you make (including your privacy settings and whether or not you are signed-in), the data you share with Cortana, and Cortana's capabilities (which vary depending on your operating system, device, and the services and apps you use). Cortana works best when you sign in and let her use data from your device, your Microsoft account, other Microsoft services, and third-party services to which you choose to connect.

You can manage what data Cortana uses, and what she knows about you in Cortana Settings, Permissions, and Notebook. More about Cortana's features and how to manage them can be found at Cortana and privacy.

The data Cortana collects is used to provide, improve, personalize, and develop Cortana and other Microsoft products. For example:

- Cortana uses information about your interests to recommend features you may enjoy.
- Cortana shares information with third parties at your direction to complete a task or transaction you've requested, such as making a restaurant reservation or booking a ride share service.
- Microsoft uses your voice data to improve speech recognition and user intent understanding to improve Cortana and other Microsoft products.

On Windows devices, if you choose not to sign in to Cortana, you can still chat with Cortana and use Cortana to search, using either your voice, inking, or typing. For more information, see the Windows Search section of this privacy statement. If you choose not to sign in to Cortana on Skype, you can still receive non-personalized suggestions and responses within Skype. See the Skype section of this privacy statement for more information.

When you use Cortana when you are signed out, we collect:

- **Voice data**. To help Cortana better understand the way you speak and your voice commands, we collect voice data and use it to build speech models and improve

speech recognition and user intent understanding. If you choose to sign in, the speech models are more personalized.

- **Searches and commands**. We collect your searches and commands to provide, improve, and develop Cortana and other products. Your Bing search queries and the Search Suggestion feature, even if Cortana does the searching for you, are treated like any other Bing search queries and are used as described in the Bing section of this privacy statement.
- **Device and usage data**. We collect information about your device as well as the hardware and software you use. For example, Cortana can access data about your device and how you use it. For instance, Cortana can determine if Bluetooth is on, whether you've locked your screen, your alarm settings, and which apps you install and use.

If you sign in with your Microsoft account, you can enable Cortana to perform additional tasks and to provide personalized experiences and suggestions. Cortana can process the demographic data (such as your age, postal code, and gender) associated with your Microsoft account and data collected through other Microsoft services to provide personalized suggestions. For example, Cortana uses data collected by the Sports app to automatically display information about the teams you follow. Cortana also learns your favorite places from the Microsoft Maps app, and what you view and purchase in Microsoft Store to improve her suggestions. Your interests in Cortana's Notebook can be used by other Microsoft services, such as Bing or MSN, to customize your interests, preferences, and favorites in those experiences as well.

When you sign in to Cortana, in addition to the information described above, we also collect:

Location data. You can choose whether Cortana processes your location information to give you the most relevant notices and results and to make suggestions that help save you time, such as local traffic information and location-based reminders. If you grant permission, Cortana will regularly collect and use your current location, location history, and other location signals (such as locations tagged on photos you upload to OneDrive). Location data Cortana collects is used to provide you with personalized experiences across our products, such as making Bing search results more relevant. It may also be used in de-identified form to improve the Windows Location Services. See more details in the Location services section of this privacy statement.

Contacts, communications, and other inputs. You can choose to let Cortana collect and access your device and cloud-based email and other communications, your calendar, and your contacts to enable additional features and personalization. If you give permission, Cortana will collect and process additional data, including:

- **Contacts, text messages, and email**. Cortana uses your contacts and messages to do a variety of things, such as: making calls when Cortana is connected to Skype, allowing you to add events to your calendar, apprising you of important messages or important contacts, and keeping you up to date on events or other things that are

important to you, like package tracking. Cortana also uses your contacts and messages to help you with planning around your events and offers other helpful suggestions and recommendations.

- **Communications history**. Cortana learns who is most important to you by analyzing your call, text message, and email history. Cortana uses this data to keep track of people most relevant to you and your preferred methods of communication, flag important messages for you (such as missed calls), and improve the performance of Cortana features, such as speech recognition.
- **Calendar appointments**. Cortana uses your calendars to provide reminders and information relevant to your appointments.

Browse history. If you choose, Cortana can use your Microsoft Edge browse history associated with your Microsoft account. Cortana uses this data to learn about you and provide you with intelligent answers and timely, personalized suggestions, or to complete web tasks for you. Cortana can also help you pick up where you left off on one device when browsing in Microsoft Edge on another device. Cortana won't collect information about sites you visit in InPrivate tabs.

Connected services and Skills. To enable greater personalization and productivity, you can give Cortana permission to (i) collect data from other Microsoft and third-party services, and (ii) share your information with those services. When you enable data sharing, Cortana shares your requests and responses with those services or third parties to enable your commands. With your permission, Cortana may also share additional information (e.g., your location). Information you share with a third party is governed by the third party's privacy policy and terms. Cortana also uses data about your use of Connected services and Skills to improve and develop Cortana and other Microsoft products. For example, we use this data, including your query sent to the third party, to improve speech recognition and user-intent understanding within Microsoft products, especially Cortana. Below are examples of how your data is processed when you use Connected services and Skills:

- If you choose to connect Cortana to your work or school account, Cortana can access data stored in Office 365 to help you stay up to date, manage your email and calendar, and get insights about your meetings and relationships.
- Choosing to sign in to LinkedIn within Cortana allows Microsoft to access your LinkedIn data so Cortana can give you more personalized information and recommendations. Please note that Cortana enables LinkedIn to access the name, email address, job title, and company name of people are you are meeting with, so she can retrieve relevant information about those contacts.
- Cortana allows you to connect to third-party services to enable her to do more and provide additional personalized experiences based upon data from the third-party service. Not all Skills require your authentication. With your permission, **Cortana can also send information about you along with your request to certain third-parties**. For instance, when you ask Cortana to request you a ride, Cortana will send Uber your request along with your current location and destination.

Microsoft Translator

Microsoft Translator is a machine translation system designed to automatically translate text and speech between numerous supported languages.

Microsoft Translator (which includes apps for Android, iOS, Windows, Presentation Translator, Translator Hub, Translator Live, Translator for Bing, and Translator for Microsoft Edge, collectively "Translator") processes the text, image, and speech data you submit, as well as device and usage data. We use this data to provide Translator, personalize your experiences, and improve our products. Microsoft has implemented business and technical measures designed to help de identify the data you submit to Translator. For example, when we randomly sample text to improve Translator, we delete identifiers and certain text, such as email addresses and some number sequences, detected in the sample that could contain personal data.

For more information on the Cognitive Services Translator Text API and Translator Speech API, see the Enterprise and developer products section of this privacy statement. For the Translate feature in Office, see the Productivity and communications products section of this privacy statement.

SwiftKey

SwiftKey Keyboard and related products (collectively, the "SwiftKey Services") process data about how you type and write, and use this data to learn your writing style and provide personalized autocorrection and predictive text that adapts to you. We also use this data to offer a range of other features, such as hashtag and emoji prediction.

SwiftKey prediction technology learns from the way you use language to build a personalized language model. This model is an optimized view of the words and phrases that you use most often in context and reflects your unique writing style. The model itself contains the words you commonly type arranged in a way to enable SwiftKey's algorithms to make predictions based on what you type. The model draws from all scenarios in which you use your keyboard, including when you type while using apps or visiting websites. The SwiftKey keyboard and model attempts to avoid collecting sensitive data, such as fields flagged as containing password or payment data. SwiftKey Services do not log, store, or learn from data you type, or the data contained in your model, unless you choose to share your data with us (as described further below). When you use SwiftKey Services, we also collect device and usage data. We use de-identified device and usage data to analyze service performance and help improve our products.

The SwiftKey Services also include an optional cloud component called a SwiftKey Account. If you choose to create a SwiftKey Account, your language model will be synced with the SwiftKey Account cloud service, so you can benefit from that model on the different devices you use and access additional services such as personalization, prediction synchronization, and backup. When you create a SwiftKey Account, Microsoft will also collect your email address and basic demographic data. All data collected is transferred to our servers over encrypted channels.

SwiftKey Account holders have the option to use the SwiftKey personalization service, which more quickly establishes and improves personalized predictions by allowing SwiftKey to access content on your device, including content you send through SMS, and certain apps such as Outlook.com, Gmail, Facebook and Twitter when you choose to connect them to the service.

You may also opt in to send short snippets of what and how you type for product improvement. To preserve your privacy, SwiftKey Services de-identifies these snippets, so they are not linked to your account. You can withdraw your consent to share these snippets at any time in SwiftKey Settings. You can also withdraw your consent to allow SwiftKey Services to use and retain your personal data at any time in SwiftKey Settings. When you withdraw consent, personal data collected through your use of the SwiftKey Services will be deleted.

You may receive occasional notifications on your device alerting you to product updates and features that may be of interest to you. You can disable these notifications at any time in the SwiftKey Settings.

Windows

Windows is a personalized computing environment that enables you to seamlessly roam and access services, preferences, and content across your computing devices from phones to tablets to the Surface Hub. Rather than residing as a static software program on your device, key components of Windows are cloud-based, and both cloud and local elements of Windows are updated regularly, providing you with the latest improvements and features. In order to provide this computing experience, we collect data about you, your device, and the way you use Windows. And because Windows is personal to you, we give you choices about the personal data we collect and how we use it. Note that if your Windows device is managed by your organization (such as your employer or school), your organization may use centralized management tools provided by Microsoft or others to control device settings, device policies, software updates, data collection by us or the organization, or other aspects of your device. For more information about data collection and privacy in Windows, see Windows 10 and your online services. Earlier versions of Windows (including Windows Vista, Windows 7, Windows 8, and Windows 8.1) are subject to their own privacy statements.

Activation

When you activate Windows, a specific product key is associated with the device on which your software is installed. The product key and data about the software and your device is sent to Microsoft to help validate your license to the software. This data may be sent again if there is a need to re-activate or validate your license. On phones running Windows, device and network identifiers, as well as device location at the time of the first power-up of the device, are also sent to Microsoft for the purpose of warranty registration, stock replenishment, and fraud prevention.

Activity history

Activity history in Windows 10 helps keep track of the things you do on your device. Activity history keeps track of the apps and services you use, the files you open, and the websites you browse—and when you do these things. Your activity history is collected and stored locally on your device, and if you've signed in to your device with a Microsoft account and given your permission, Windows sends your activity history to Microsoft. Once your activity history is in the cloud, Microsoft uses that data to enable cross-device experiences, to provide you with personalized experiences and relevant suggestions, and to help improve Microsoft products.

Activity history is also created and sent to Microsoft when you use Microsoft apps, such as Microsoft Edge, and Office apps like Word, Excel, and PowerPoint, on mobile devices such as iOS and Android phones and tablets. If you are signed in with your Microsoft account, you can continue activities on your PC that you started in Microsoft apps on your Android or iOS device.

Advertising ID

Windows generates a unique advertising ID for each user on a device. When the advertising ID is enabled, apps (both Microsoft apps and third-party apps) can access and use the advertising ID in much the same way that websites can access and use a unique identifier stored in a cookie. Thus, your advertising ID can be used by app developers and advertising networks to provide more relevant advertising and other personalized experiences across their apps and on the web. Microsoft collects the advertising ID for the uses described here only when you choose to enable the advertising ID as part of your privacy setting. You can turn off access to this identifier at any time by turning off the advertising ID in your privacy settings (in **Start** > **Settings** > **Privacy**). If you choose to turn it on again, the advertising ID will be reset and a new identifier will be generated. When a third-party app accesses the advertising ID, its use of the advertising ID will be subject to its own privacy policy. For more information on the use of data for advertising by Microsoft, see the How we use personal data section of this statement.

Diagnostics

Microsoft collects Windows diagnostic data to solve problems and to keep Windows up to date, secure, and operating properly. It also helps us improve Windows and related Microsoft products and services and, for users who have turned on “Tailored experiences,” to provide more relevant tips and recommendations to tailor Microsoft and third-party products and services for Windows to the user’s needs. 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. There are two levels of diagnostic and usage data: **Basic** and **Full**.

Basic data includes information about your device, its settings and capabilities, and whether

it is performing properly. We collect the following data at the Basic level:

- Device, connectivity, and configuration data:
  - Data about the device such as the processor type, OEM manufacturer, type of battery and capacity, number and type of cameras, firmware, and memory attributes.
  - Network capabilities and connection data such as the device's IP address, mobile network (including IMEI and mobile operator) and whether the device is connected to a free or paid network.
  - Data about the operating system and its configuration such as the OS version and build number, region and language settings, diagnostics level, and whether the device is part of the Windows Insider program.
  - Data about connected peripherals such as model, manufacturer, drivers, and compatibility data.
  - Data about the applications installed on the device such as application name, version, and publisher.
- Whether a device is ready for an update and whether there are factors that may impede the ability to receive updates, such as low battery, limited disk space, or connectivity through a paid network.
- Whether updates complete successfully or fail.
- Data about the reliability of the diagnostics collection system itself.
- Basic error reporting, which is health data about the operating system and applications running on your device. For example, basic error reporting tells us if an application, such as Microsoft Paint or a third-party game, hangs or crashes.

Full data includes everything collected with Basic data, plus additional information about device health, device usage, and enhanced error reporting that helps Microsoft to fix and improve products and services for all users. We collect the following additional information at the Full level:

- Additional data about the device, connectivity, and configuration, beyond that collected at Basic.
- Status and logging information about the health of operating system and other system components (in addition to data about the update and diagnostics systems collected at Basic).
- App usage, such as which programs are launched on a device, how long they run, and how quickly they respond to input.
- Browser usage, including browsing history and search terms, in Microsoft browsers (Microsoft Edge or Internet Explorer).
- Enhanced error reporting, including the memory state of the device when a system or app crash occurs (which may unintentionally contain user content, such as parts of a file you were using when the problem occurred). Crash data is never used for Tailored experiences as described below.

Some of the data described above may not be collected from your device even if your diagnostic data setting is set to Full. Microsoft minimizes the volume of data it collects from

all devices by collecting some of the data at the Full level from only a subset of devices (sample). By running the Diagnostic Data Viewer tool, 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 at **Start** > **Settings** > **Privacy** > **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 10 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 at both levels of diagnostics, see Windows 10 diagnostic data at the Full level or Windows 10 diagnostic data at the Basic level for the current list of data collected at Basic. We provide limited portions of error report information to partners (such as OEMs) to help them troubleshoot products and services which work with Windows and other Microsoft product and services. They are only permitted to use this information to repair or improve those products and services.

Inking and typing Recognition. You also can choose to help Microsoft improve inking and typing recognition by sending inking and typing diagnostic data. If you choose to do so, 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 in the many languages used by Windows customers. 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.

If you choose to turn on **Tailored experiences**, we will use your Windows diagnostic data (Basic or Full as you have selected) to offer you personalized tips, ads, and recommendations to enhance Microsoft products and services for your needs. If you have selected Basic 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 Full, personalization is also based on information about the websites you browse, how you use apps and features, plus additional information about device health. However, we do not use the content of crash dumps for personalization when we receive such data from users who have selected Full.

Tailored experiences include suggestions on how to customize and optimize Windows; and recommendations for and offers of 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. If you stream movies in your browser, you may be recommended an app from the Microsoft Store that

streams more efficiently. 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.

Location services, motion sensing, and recording

Windows location service. Microsoft operates a location service that helps determine the precise geographic location of a specific Windows device. Depending on the capabilities of the device, location is determined using Global Navigation Satellite Systems (for example GPS); detecting nearby cell towers and/or Wi-Fi access points and comparing that information against a database that Microsoft maintains of cell towers and Wi-Fi access points whose location is known; or deriving location from your device's IP address. When the location service is active on a Windows device, or you have given permission for Microsoft apps to access location information on non-Windows devices, data about cell towers and Wi-Fi access points and their locations is collected by Microsoft and added to the location database after removing any data identifying the person or device from which it was collected. Microsoft may also share this de-identified location data with third parties to provide and improve location and mapping services.

Windows services and features (such as browsers and Cortana), applications running on Windows, and websites opened in Windows browsers can access the Windows location service to determine precise location if you allow them to do so. Some features and apps request precise location permission when you first install Windows, some ask the first time you use the app, and others ask every time you access the location service. For information about certain Windows apps that use the location service, see the Windows apps section of this privacy statement.

When the location service is accessed, your Windows device will also upload its location to Microsoft, and we will retain only the last known location (each new location replaces the previous one) to improve the efficiency and operation of our services. Data about a Windows device's recent location history is stored on the device, and certain apps and Windows features can access this location history. You can clear your device's location history at any time in the device's Settings menu.

In Settings, you can also view which applications have access to the location service or your device's location history, turn off or on access to the location service for particular applications, or turn off the location service. You can also set a default location, which will be used when the location service can't detect a more exact location for your device.

Note that on mobile devices, your mobile operator will have access to your location even if you turn off the location service.

General Location. If you turn on the General Location feature, apps that cannot use your precise location will have access to your general location, such as your city, postal code, or region.

Find My Phone. The Find My Phone feature allows you to find the location of your

Windows phone from the Microsoft account website, even if you have turned off all access to the location service on the phone. If you have turned on the "save my location every few hours" feature in the Find My Phone settings on your phone, the Find My Phone feature will periodically send and store a single last-known location of your phone, even if you have turned off location services on your phone. Each time a new location is sent, it replaces the previously-stored location.

Find my device. The Find my device feature allows an administrator of a Windows PC or tablet to find the location of that device if the administrator has enabled the location service for the device, even if other users have disabled location for themselves. When the administrator attempts to locate the device, users will see a notification in the notification center.

Windows motion sensing. Windows devices with motion activity detection can collect motion activity. This data can enable features such as a pedometer to count the number of steps you take, so a fitness application can estimate how many calories you burn. This data and history is stored on your device and can be accessed by applications you give permission to access and use that data.

Recording. Some Windows devices have a recording feature that allows you to capture audio and video clips of your activity on the device, including your communications with others. If you choose to record a session, the recording will be saved locally on your device. In some cases, you may have the option to transmit the recording to a Microsoft product or service that broadcasts the recording publicly. **Important: You should understand your legal responsibilities before recording and/or transmitting any communication. This includes whether you need to get consent from all parties to the communication in advance**. Microsoft is not responsible for how you use recording features or your recordings.

Security and safety features

Device encryption. Device encryption helps protect the data stored on your device by encrypting it using BitLocker Drive Encryption technology. When device encryption is on, Windows automatically encrypts the drive Windows is installed on and generates a recovery key. The BitLocker recovery key for your personal device is automatically backed up online in your personal Microsoft OneDrive account. Microsoft doesn't use your individual recovery keys for any purpose.

Malicious Software Removal Tool. The Malicious Software Removal Tool (MSRT) runs on your device at least once per month as part of Windows Update. MSRT checks devices for infections by specific, prevalent malicious software ("malware") and helps remove any infections found. When the MSRT runs, it will remove the malware listed on the Microsoft Support website if the malware is on your device. During a malware check, a report will be sent to Microsoft with specific data about malware detected, errors, and other data about your device. If you do not want MSRT to send this data to Microsoft, you can disable MSRT's reporting component.

Microsoft Family. Parents can use Microsoft Family to understand and set boundaries on how their child is using their device. There are many features available to Family members, so please carefully review the information provided when you create or join a Family. When Family activity reporting is turned on for a child, Microsoft will collect details about how the child uses their device and provide parents with reports of that child's activities. Activity reports are routinely deleted from Microsoft servers after a short period of time.

Windows Defender SmartScreen. Windows Defender SmartScreen helps protect you when using our services by checking downloaded files and web content for malicious software, potentially unsafe web content, and other threats to you or your device. When checking a file, data about that file is sent to Microsoft, including the file name, a hash of the file's contents, the download location, and the file's digital certificates. If Windows Defender SmartScreen identifies the file as unknown or potentially unsafe, you will see a warning prior to opening the file. When checking web content, data about the content and your device is sent to Microsoft, including the full web address of the content. If Windows Defender SmartScreen detects that content is potentially unsafe, you will see a warning in place of the content. Windows Defender SmartScreen can be turned on or off in Settings.

Windows Defender Antivirus. Windows Defender Antivirus looks for malware and other unwanted software on your device. Windows Defender Antivirus is automatically turned on to help protect your device if no other antimalware software is actively protecting your device. If Windows Defender Antivirus is turned on, it will monitor the security status of your device. When Windows Defender Antivirus is turned on, or is running because Limited Periodic Scanning is enabled, it will automatically send reports to Microsoft that contain data about suspected malware and other unwanted software, and it may also send files that could contain malware. If a report is likely to contain personal data, the report is not sent automatically, and you'll be prompted before it is sent. You can configure Windows Defender Antivirus not to send reports and suspected malware to Microsoft.

Speech recognition

Windows provides both a device-based speech recognition feature (available through the Windows Speech Recognition Desktop app), and a cloud-based speech recognition service in regions where Cortana is available. To find out which languages and regions speech currently supports, see Cortana's regions and languages. When you use cloud-based speech recognition, Microsoft collects and uses your voice input to provide you with speech recognition services in Cortana, in the Mixed Reality Portal, in supported Microsoft Store applications, dictation in Windows, and over time in other parts of Windows. The voice data is used in the aggregate to help improve our ability to correctly recognize all users' speech.

If you've given permission in Cortana, we also collect your name and nickname, your recent calendar events, and the names of the people in your appointments, information about your contacts including names and nicknames, names of your favorite places, apps you use, and information about your music preferences. This additional data enables us to better recognize people, events, places, and music when you dictate commands, messages, or

documents.

If you turn off the speech services and typing suggestions setting, this will stop the data collection for cloud speech recognition.

Sync settings

When you sign in to Windows with a Microsoft account, Windows syncs some of your settings and data with Microsoft servers to make it easier to have personalized experiences across multiple devices. After you've signed in to one or more devices with a Microsoft account, when you sign in to another with the same Microsoft account for the first time, Windows will download and apply the settings and data you choose to sync from your other devices. Settings you choose to sync will automatically update on Microsoft servers and your other devices as you use them.

Some of the settings that are synced include:

- Apps you've installed from the Microsoft Store
- Language preferences
- Ease of Access preferences
- Personalization settings such as your account picture, background, and mouse settings
- Settings for Microsoft Store apps
- Spell-checker dictionaries, input method editor (IME) dictionaries, and personal dictionaries
- Internet Explorer browser history, favorites, and websites you have open
- Saved app, website, mobile hotspot, and Wi-Fi network names and passwords

You can choose whether to sync your settings, and control what is synced, by going to **Start** > **Settings** > **Accounts** > **Sync your settings**. Some apps have their own, separate sync controls. If you sign in to Windows with a work account and you choose to connect that account to your personal Microsoft account, Windows will ask which settings you want to sync before connecting your Microsoft account.

Update Services

Update Services for Windows includes Windows Update and Microsoft Update. Windows Update is a service that provides you with software updates for Windows software and other supporting software, such as drivers and firmware supplied by device manufacturers. Microsoft Update is a service that provides you with software updates for other Microsoft software such as Office.

Windows Update automatically downloads Windows software updates to your device. You can configure Windows Update to automatically install these updates as they become available (recommended) or have Windows notify you when a restart is required to finish installing updates. Apps available through the Microsoft Store are automatically updated

through the Microsoft Store, as described in the Microsoft Store section of this privacy statement.

Web browsers—Microsoft Edge and Internet Explorer

Microsoft Edge is the default web browser for Windows. Internet Explorer, the legacy browser from Microsoft, is also available in Windows. Whenever you use a web browser to access the internet, data about your device ("standard device data") is sent to the websites you visit and online services you use. Standard device data includes your device's IP address, browser type and language, access times, and referring website addresses. This data might be logged on those websites' web servers. Which data is logged and how that data is used depends on the privacy practices of the websites you visit and web services you use.

Additionally, data about how you use your browser, such as your browsing history, web form data, temporary internet files, and cookies, is stored on your device. You can delete this data from your device using Delete Browsing History.

Microsoft Edge allows you to capture and save content on your device, such as:

- **Web note**. Allows you to create ink and text annotations on the webpages you visit, and clip, save, or share them.
- **Active reading**. Allows you to create and manage reading lists, including websites or documents.
- **Hub**. Allows you to easily manage your reading lists, favorites, downloads, and history all in one area.

Some Microsoft browser information saved on your device will be synced across other devices when you sign in with your Microsoft account. For instance, in Internet Explorer, this information includes your browsing history and favorites; and in Microsoft Edge, it includes your favorites, reading lists, autofill form entries (such as your name, address, and phone number), and may include data for extensions that you have installed. As an example, if you sync your Microsoft Edge reading list across devices, copies of the content you choose to save to your reading list will be sent to each synced device for later viewing. You can disable syncing in Internet Explorer by going to **Start** > **Settings** > **Accounts** > **Sync your settings**. (For more information, see the Sync settings section of this privacy statement.) You can also disable syncing of Microsoft Edge browser information by turning off the sync option in Microsoft Edge Settings.

Microsoft Edge and Internet Explorer use your search queries and browsing history to provide you with faster browsing and more relevant search results. These features include:

- **Search suggestions** in Internet Explorer automatically sends the information you type into the browser address bar to your default search provider (such as Bing) to offer search recommendations as you type each character.
- **Search and site suggestions** in Microsoft Edge automatically sends the information

you type into the browser address bar to Bing (even if you have selected another default search provider) to offer search recommendations as you type each character.

You can turn off these features at any time. In order to provide search results, Microsoft Edge and Internet Explorer send your search queries, standard device information, and location (if you have location enabled) to your default search provider. If Bing is your default search provider, we use this data as described in the Bing section of this privacy statement.

Cortana can assist you with your web browsing in Microsoft Edge with features such as Ask Cortana. You can disable Cortana assistance in Microsoft Edge at any time in Microsoft Edge Settings. To learn more about how Cortana uses data and how you can control that, go to the Cortana section of this privacy statement.

Windows apps

A number of Microsoft apps are included with Windows and others are available in Microsoft Store. Some of those apps include:

Maps app. The Maps app provides location-based services and uses Bing services to process your searches within the Maps app. When the Maps app has access to your location, and you have enabled location-based services in Windows, when you use the “@” key to initiate a search in supported text boxes in Windows apps, Bing services collects the text you type after the “@” key to provide location-based suggestions. To learn more about these Bing-powered experiences, see the Bing section of this privacy statement. When the Maps app has access to your location, even when the app is not in use, Microsoft may collect de-identified location data from your device to improve Microsoft services. You can disable the Maps app's access to your location by turning off the location service or turning off the Maps app's access to the location service.

You can keep track of your favorite places and recent map searches in the Maps app. Your favorite places and search history will be included as search suggestions. If you're signed in with your Microsoft account, your favorite places, search history, and certain app settings will be synced across other devices and services (for example, Cortana). For more information, see the Sync settings section of this privacy statement.

Camera and Photo apps. If you allow the Camera app to use your location, location data is embedded in the photos you take with your device. Other descriptive data, such as camera model and the date that the picture was taken, is also embedded in photos and videos. If you choose to share a photo or video, any embedded data will be accessible to the people and services you share with. You can disable the Camera app's access to your location by turning off all access to the location service in your device's Settings menu or turning off the Camera app's access to the location service.

Your photos, videos, and screenshots that are saved in your camera roll automatically upload to OneDrive. You can manage your photos and videos in OneDrive, and you can

disable the automatic upload in Settings.

When you take photos embedded with your location, the Photos app can group your photos by time and location. To group your photos, the Photos app sends location data in your photos to Microsoft to determine the names of locations, such as "Seattle, Washington." When you are using the Photo app while signed in to your Microsoft account, your photos and videos from OneDrive will be automatically sorted into albums in the Photo app and will also appear on the Photo app's live tile. Your photos and/or videos will only be shared with others if you choose to do so.

People app. The People app lets you see and interact with all your contacts in one place. When you add an account to the People app, your contacts from your account will be automatically added to the People app. You can add other accounts to the People app, including your social networks (such as Facebook and Twitter) and email accounts. When you add an account, we tell you what data the People app can import or sync with the particular service and let you choose what you want to add. Other apps you install may also sync data to the People app, including providing additional details to existing contacts. When you view a contact in the People app, information about your recent interactions with the contact (such as emails and calendar events, including from apps that the People app syncs data from) will be retrieved and displayed to you. You can remove an account from the People app at any time.

Mail and Calendar app. The Mail and Calendar app allows you to connect all your email, calendars, and files in one place, including those from third-party email and file storage providers. The app provides location-based services, such as weather information in your calendar, but you can disable the app's use of your location. When you add an account to the Mail and Calendar app, your email, calendar items, files, contacts, and other settings from your account will automatically sync to your device and to Microsoft servers. At any time, you can remove an account or make changes to the data that's synced from your account. To configure an account, you must provide the app with the account credentials (such as user name and password), which will be sent over the internet to the third-party provider's server. The app will first attempt to use a secure (SSL) connection to configure your account but will send this information unencrypted if your email provider does not support SSL. If you add an account provided by an organization (such as a company email address), the owner of the organizational domain can implement certain policies and controls (for example, multi-factor authentication or the ability to remotely wipe data from your device) that may affect your use of the app.

Messaging app. When you sign in with a Microsoft account on your device, you can choose to back up your information, which will sync your SMS and MMS messages and store them in your Microsoft account. This allows you to retrieve the messages if you lose or change phones. After your initial device set-up, you can manage your messaging settings at any time. Turning off your SMS/MMS backup will not delete messages that have been previously backed up to your Microsoft account. To delete such messages, you must first delete them from your device prior to turning off backup. If you allow the Messaging app to use your location, you can attach a link to your current location to an outgoing message.

Location information will be collected by Microsoft as described in the Windows Location services section of this privacy statement.

Microsoft Wallet app for Windows Phone. You can use Microsoft Wallet to hold information such as coupons, loyalty cards, tickets, and other digital content. Where available, you can also add payment cards to the Microsoft Wallet to make payments at participating stores using NFC (near-field communication).

You can set up your wallet for payment by signing in to Microsoft Wallet with your personal Microsoft account and adding payment cards associated with your Microsoft account. When you add a payment card to Microsoft Wallet, we provide data to your bank and payment card network, including your name, card number, billing address, email address, device data (including the device name, type, and identifier), and your location at the time you add your payment card to your wallet. This data is sent to your bank and payment card network to determine the eligibility of your payment card, enable transactions, and detect fraud.

When you make an NFC payment, Microsoft Wallet will provide the merchant with an encrypted version of your payment card (a “token”). The merchant will present this token, along with transaction details, to your bank to complete the transaction and request payment for your transaction.

Windows Media Player

Windows Media Player allows you to play CDs, DVDs, and other digital content (such as WMA and MP3 files), rip CDs, and manage your media library. To enrich your experience when you play content in your library, Windows Media player displays related media information, such as album title, song titles, album art, artist, and composer. To augment your media information, Windows Media player will send a request to Microsoft which contains standard computer information, an identifier for the media content, and the media information already contained in your Windows Media Player library (including information you may have edited or entered yourself) so that Microsoft can recognize the track and then return additional information that is available.

Windows Media Player also allows you to play back content that is streamed to you over a network. To provide this service, it is necessary for Windows Media Player to communicate with a streaming media server. These servers are typically operated by non-Microsoft content providers. During playback of streaming media, Windows Media Player will send a log to the streaming media server or other web server(s) if the streaming media server requests it. The log includes such details as: connection time, IP address, operating system version, Windows Media Player version, Player identification number (Player ID), date, and protocol. To protect your privacy, Windows Media Player defaults to sending a Player ID that is different for each session.

Windows Hello

Windows Hello provides instant access to your devices through biometric authentication. If you turn it on, Windows Hello uses your face, fingerprint, or iris to identify you based on a set of unique points or features that are extracted from the image and stored on your device as a template—but it does not store the actual image of your face, fingerprint, or iris. Biometric verification data that's used when you sign in doesn't leave your device. You can delete your biometric verification data from within Settings.

Windows Search

Windows Search lets you search your stuff and the web from one place. If you choose to use Windows Search to search "your stuff," it will provide results for items on your personal OneDrive, your OneDrive for Business if so enabled, other cloud storage providers to the extent supported by those third-party providers, and on your device. If you choose to use Windows Search to search the web, or get search suggestions with Windows Search, your search results will be powered by Bing and we will use your search query as described in the Bing section of this privacy statement.

Entertainment and related services

Entertainment and Related Services power rich experiences and enable you to access a variety of content, applications and games.

Xbox and Xbox Live

Xbox consoles are hardware devices that you can use to access and play games, movies, music, and other forms of digital entertainment. Xbox Live is the online gaming and entertainment service from Microsoft that enables you to find content and connect with friends, on Xbox Live and other gaming and social networks, from a variety of devices, including Xbox consoles.

When you access an Xbox experience from a device, we assign you a unique device identifier. When your Xbox console is connected to the internet, we identify which console and which version of the Xbox operating system you are currently using. When you sign up for Xbox Live, we assign an Xbox user ID and a gamertag (a nickname) to identify you. Data we collect about your use of Xbox Live is stored with these unique identifier(s).

We collect data about your use of Xbox and Xbox Live, such as:

- When you sign in and sign out of Xbox Live, the games you play and apps you use, your game progress and play statistics, the purchases you make, and content you obtain.
- Performance data about Xbox consoles and Xbox Live, connected devices, and your network connection, including software or hardware errors.
- Content you add, upload, or share through Xbox Live, including text, images and video from within games or apps.

- Social activity, including your interactions with other gamers, and your connections, including friends and followers, on Xbox Live.
- If you use the Xbox console with Kinect, data about how you use Kinect. See below for more information about Kinect data collection.
- If you use the Xbox TV app, we collect TV viewing history from your console in a way that doesn't identify you or others.

With your consent, we will collect information about videos you purchase or view through third-party apps on your Xbox console. If you use an Xbox console that includes a storage device (hard drive or memory unit), and if you play offline or have never signed in to Xbox Live on the console, usage data will be stored on the storage device and sent to Microsoft the next time you sign in.

Microsoft uses the data we collect from Xbox and Xbox Live to provide you with Xbox experiences, which includes securing the services and carrying out the transactions you request. We also use the data to improve and develop our products. As part of the Xbox Live service, Microsoft will also use data about you and your use of Xbox Live (such as the games you play, apps you use, subscriptions you have, purchases you make, and content you obtain) to provide you with a personalized, highly curated gaming and entertainment experience. This includes connecting you to games, content, and services, as well as presenting you with offers, discounts, and recommendations.

Xbox Live data viewable by other users. Your gamertag, game and play statistics, achievements, presence (whether you're currently signed in to Xbox Live), content you share, and other data about your activity on Xbox Live can be seen by other users on Xbox Live, users of third-party services you have linked your profile to, or on other properties associated with Xbox Live (including those of partner companies). For example, your gamertag and scores that show on game leaderboards are considered public and can't be hidden. For other data, like presence, you can adjust your privacy settings on the console or at xbox.com to limit or block sharing with the public or even with friends.

Xbox Live data shared with game or app publishers. When you use an Xbox Live-enabled game or any network-connected app through your Xbox console, the publisher for that game or app has access to data about your usage of Xbox Live and its game or app so it may deliver and improve its product and provide support. This data may include your Xbox user ID and gamertag, limited account information such as country and age range, data about your in game communications, enforcement activity, game-play sessions (for example, moves made in-game, types of vehicles used in-game), your presence on Xbox Live, the time you spend playing the game or app, rankings, statistics, gamer profiles, avatars or gamerpics, friends lists, activity feed, club memberships, and content that you may create or submit within the game or app. Third-party game and app publishers are independent controllers of this data and its use is subject to their privacy policies. You should carefully review their policies to determine how they will use the data. For example, publishers may choose to disclose or display game data (such as on leaderboards) through their own services. To learn more about our data-sharing practices with third-party publishers, see Data Sharing with Games and Apps.

Linking your Xbox Live profile to non-Microsoft accounts. Some games or apps available through Xbox Live, and some social features of Xbox Live, are delivered by third-party publishers or partner companies, which may require that you create a non-Microsoft account and sign-in credentials to use that game, app, or feature. If you choose to link your Xbox Live profile with an account of a third-party publisher or partner company, we will share with them limited account and profile information but will not include any credit card or other payment information.

Kinect. The Kinect sensor is a combination of camera, microphone, and infrared sensor that can enable motions and voice to be used to control gameplay and to navigate through the service. For example:

- If you choose, the camera can be used to sign you in to the service automatically using facial recognition. To do this, it takes an image of your face and measures distances between key points to create and store a numeric value that represents only you. This data stays on the console and is not shared with anyone, and you can choose to delete this data from your console at any time.
- For gameplay, Kinect will map distances between your body's joints to create a stick figure representation of you that helps Kinect enable gameplay. If you are playing online, we collect those numeric values to enable and improve gameplay and the gaming experience. Kinect also detects specific hand gestures intended to do simple system interactions (such as menu navigation, pan/zoom, and scroll).
- For some fitness games, Xbox can use the Kinect sensor to estimate your exercise data, including estimates such as your heart rate during a certain activity or the number of calories burned during a workout.
- Kinect's microphones enable voice chat between players during gameplay. They also enable voice commands for control of the console, game, or app, or to enter search terms. See below for additional details on voice data collection.
- The Kinect sensor can also be used for audio and video communications through services such as Skype.

To learn more about Kinect, for Xbox 360, see Kinect and Xbox 360 privacy. For Xbox One, see Kinect and Xbox One Privacy.

Captioning. During Xbox Live real-time chat, players may activate a voice-to-text feature, which allows the user to view the audio in-game chat as text. If a user activates this feature, the other players will have no additional notice. Microsoft uses this data to provide captioning of chat for users who need it as well as the other purposes described in this privacy statement.

Communications monitoring. Xbox Live includes communications features such as text and voice direct messaging and real-time text and voice chat. In order to help provide a safe gaming environment and enforce the Microsoft Code of Conduct, we collect and monitor direct messaging, and text communications in live-hosted multiplayer gameplay sessions and other features of the service, such as activity feeds and clubs.

Voice data for service improvement. We collect and use for service improvement voice search requests or samples of voice commands occurring while using Kinect or Cortana. This data is stored separately from your Xbox profile.

GameDVR. Any player in a multiplayer game session can use GameDVR to record their view of the gameplay taking place in that session. The recording can capture your in-game character and gamertag in the game clips created by other players in the gameplay session. Note that if a player uses GameDVR on a PC, audio chat may also be captured in a game clip.

Children and online safety. If you have children or teenagers who use Xbox Live, you can set up child and teen profiles for them. Children and teens under 18 cannot create a profile on Xbox Live without parental consent. Adults in the family can change consent choices and online safety settings for child and teen profiles on xbox.com.

Microsoft Store

Microsoft Store is an online service that allows you to browse, download, purchase, rate, and review applications and other digital content. It includes:

- Apps and content for Windows devices such as phones, PCs, and tablets.
- Games and other apps for Xbox consoles.
- Products and apps for Office, SharePoint, Exchange, Access, and Project (2013 versions or later).

We collect data about how you access and use Microsoft Store; the products you've viewed, purchased, or installed; the preferences you set for viewing apps in Microsoft Store; and any ratings, reviews, or problem reports you submit. Your Microsoft account is associated with your ratings and reviews; and if you write a review, the name and picture from your Microsoft account will be published with your review.

Permission for Microsoft Store apps. Many apps you install from the Microsoft Store are designed to take advantage of specific hardware and software features of your device. An app's use of certain hardware and software features may give the app or its related service access to your data. For example, a photo editing app might access your device's camera to let you take a new photo or access photos or videos stored on your device for editing, and a restaurant guide might use your location to provide nearby recommendations. Information about the features that an app uses is provided on the app's product description page in Microsoft Store. Many of the features that Microsoft Store apps use can be turned on or off through your device's privacy settings. In Windows, in many cases, you can choose which apps can use a particular feature. Go to **Start > Settings > Privacy,** select the feature (for example, Calendar), and then select which app permissions are on or off. The lists of apps in Windows privacy settings that can use hardware and software features will not include "Classic Windows" applications, and these applications are not affected by these settings.

App updates. Unless you have turned off automatic app updates in the relevant Microsoft Store settings, Microsoft Store will automatically check for, download, and install app updates to ensure that you have the latest versions. Updated apps might use different Windows hardware and software features from the previous versions, which could give them access to different data on your device. You will be prompted for consent if an updated app accesses certain features, such as location. You can also review the hardware and software features an app uses by viewing its product description page in Microsoft Store.

Each app's use of your data collected through any of these features is subject to the app developer's privacy policies. If an app available through Microsoft Store collects and uses any of your personal data, the app developer is required to provide a privacy policy, and a link to the privacy policy is available on the app's product description page in Microsoft Store.

Sideloaded apps and developer mode. Developer features such as the "developer mode" setting are intended for development use only. If you enable developer features, your device may become unreliable or unusable, and expose you to security risks. Downloading or otherwise acquiring apps from sources other than Microsoft Store, also known as "sideloading" apps, may make your device and personal data more vulnerable to attack or unexpected use by apps. Windows policies, notifications, permissions, and other features intended to help protect your privacy when apps access your data may not function as described in this statement for sideloaded apps or when developer features are enabled.

MSN

MSN services include websites and a suite of apps, including MSN News, Weather, Sports, and Money, and previous versions of the apps branded as Bing (together, "MSN Apps"). The MSN Apps are available on various platforms, including Windows, iOS, and Android. MSN services are also included within other Microsoft services, including the Microsoft Edge browser.

When you install MSN Apps, we collect data that tells us if the app was installed properly, the installation date, the app version, and other data about your device such as the operating system and browser. This data is collected on a regular basis to help us determine the number of MSN App users and identify performance issues associated with different app versions, operating systems, and browsers.

We also collect data about how you interact with MSN services, such as usage frequency and articles viewed, to provide you with relevant content. Some MSN services provide an enhanced experience when you sign in with your Microsoft account, including allowing you to customize your interests and favorites. You can manage personalization through MSN and Bing settings, as well as through settings in other Microsoft services that include MSN services. We also use the data we collect to provide you with advertisements that may be of interest to you. You can opt out of interest-based advertising through the advertising links within MSN services, or by visiting the Microsoft opt-out page.

Previous versions of MSN Money allow you to access personal finance information from third-party financial institutions. MSN Money only displays this information and does not store it on our servers. Your sign-in credentials used to access your financial information from third parties are encrypted on your device and are not sent to Microsoft. These financial institutions, as well as any other third-party services you access through MSN services, are subject to their own terms and privacy policies.

Mixer

Mixer is an interactive, social, online service for live streaming videos, videogames, and related content.

Mixer collects data from you to provide the service, including the third-party experiences you choose, improve our products, communicate with you, and show you advertising. Specifically, Mixer collects account data (including the content of your public profile), content (such as streams), and device and usage data. If you stream your content on the service, then your content and any personal information you include in your content will be public and may be captured and shared by others. Note that Microsoft may review and reject any content you stream or store on the service for violations of the Mixer Rules of User Conduct or the Microsoft Code of Conduct.

Some of the apps and experiences on Mixer are provided by third-party developers. When you choose to use third-party apps or experiences: (i) your data is subject to that third party's privacy policy; and (ii) Microsoft may share non-public additional information about your Mixer profile and Microsoft account with that developer. This information can include your settings, email, age, and other information you provide.

Groove Music and Movies & TV

Groove Music lets you easily play your music collection and make playlists. Microsoft Movies & TV allows you to play your video collection and rent or buy movies and TV episodes. These services were formerly offered as Xbox Music and Video.

To help you discover content that may interest you, Microsoft will collect data about what content you play, the length of play, and the rating you give it. If you sign in to Cortana on your device, Microsoft will collect and use data related to the music you play via Groove Music to provide personalized experiences and relevant suggestions.

To enrich your experience when playing content, Groove Music and Movies & TV will display related information about the content you play and the content in your music and video libraries, such as the album title, cover art, song or video title, and other information, where available. To provide this information, Groove Music and Movies & TV send an information request to Microsoft containing standard device data, such as your device IP address, device software version, your regional and language settings, and an identifier for the content.

If you use Movies & TV to access content that has been protected with Microsoft Digital Rights Management (DRM), it may automatically request media usage rights from an online rights server and download and install DRM updates in order to let you play the content. See the DRM information in the Silverlight section of this privacy statement for more information.

Silverlight

Microsoft Silverlight helps you to access and enjoy rich content on the Web. Silverlight enables websites and services to store data on your device. Other Silverlight features involve connecting to Microsoft to obtain updates, or to Microsoft or third-party servers to play protected digital content.

Silverlight Configuration tool. You can make choices about these features in the Silverlight Configuration tool. To access the Silverlight Configuration tool, right click on content that is currently being displayed by Silverlight and select **Silverlight**. You can also run the Silverlight Configuration tool directly. In Windows, for example, you can access the tool by searching for "Microsoft Silverlight."

Silverlight application storage. Silverlight-based applications can store data files locally on your computer for a variety of purposes, including saving your custom settings, storing large files for graphically intensive features (such as games, maps, and images), and storing content that you create within certain applications. You can turn off or configure application storage in the Silverlight Configuration tool.

Silverlight updates. Silverlight will periodically check a Microsoft server for updates to provide you with the latest features and improvements. A small file containing information about the latest Silverlight version will be downloaded to your computer and compared to your currently installed version. If a newer version is available, it will be downloaded and installed on your computer. You can turn off or configure updates in the Silverlight Configuration tool.

Digital Rights Management. Silverlight uses Microsoft Digital Rights Management (DRM) technology to help protect the rights of content owners. If you access DRM-protected content (such as music or video) with Silverlight, it will request media usage rights from a rights server on the Internet. In order to provide a seamless playback experience, you will not be prompted before Silverlight sends the request to the rights server. When requesting media usage rights, Silverlight will provide the rights server with an ID for the DRM-protected content file and basic data about your device, including data about the DRM components on your device such as their revision and security levels, and a unique identifier for your device.

DRM updates. In some cases, accessing DRM-protected content will require an update to Silverlight or to the DRM components on your device. When you attempt to play content that requires a DRM update, Silverlight will send a request to a Microsoft server containing basic data about your device, including information about the DRM components on your

computer such as their revision and security levels, troubleshooting data, and a unique identifier for your device. The Microsoft server uses this identifier to return a unique DRM update for your device, which will then be installed by Silverlight. You can turn off or configure DRM component updates on the **Playback** tab in the Silverlight Configuration tool.

Microsoft Health services

Microsoft Health services can help you understand and manage your health data. They include HealthVault, HealthVault Insights, Microsoft Band devices, other Microsoft Health applications and related products. The Band helps you keep track of data like heart rate and steps taken. The Band can also use Cortana to take notes and receive notifications from your phone. The Microsoft Health applications send data to Microsoft servers and allow you to view, manage and control the data. The applications may enable notifications to the Band and other devices. HealthVault services let you gather, edit, add to, and store health data online, and share your health data with family, caregivers, and health care professionals.

Microsoft Health services collect and use your data to provide the services, which includes improving and personalizing your experiences. Health data you provide to Microsoft through Microsoft Health services is not combined with data from other Microsoft services, or used for other purposes without your explicit consent. For example, Microsoft does not use your health record data to market or advertise to you without your opt-in consent.

Health services

Microsoft Health services can help you understand and manage your health data. The data collected depends on the services and features you use, and includes the following:

- **Profile data**. When you create a profile, you provide data, such as height, weight, and age that is used to calculate your activity results. Other profile data comes from your personal Microsoft account.
- **Activity and fitness data**. Microsoft Health services help you keep track of your activity and fitness by collecting data like your heart rate, steps, calories burned, and sleep. Examples of types of activities you can choose to track are runs, workouts, and sleep.
- **Usage data**. To provide you with the best service, we collect and automatically upload statistics about the performance and your use of the Microsoft Health services.
- **Location**. Microsoft Band has built-in Global Positioning System (GPS) capabilities, which let you map your activities like running or biking, without having to carry your phone with you. If you enable GPS for an activity, you can view the activity map in the Microsoft Health applications. Some modes on the Band, such as Golf and Explorer, automatically turn on GPS, and turn it off when you end the mode.

To learn more about the Band's sensors and the data they collect, see the Microsoft Band page on the Microsoft Support website.

Access and control. You can view and manage your data in Microsoft Health services. For example, you can view and update your profile data, manage connected applications, and view past activities. You can delete specific activity details in the Microsoft Health services. When you delete a specific activity, the event is deleted from the Microsoft Health services; however, other data and the basic sensor data captured by the devices remain in the Microsoft Health services. You can cancel your Microsoft Health services account at any time by contacting Customer Support from the Microsoft Band website.

Cortana. The Microsoft Health services allow you to use Cortana. When you use Cortana, data you process in the Microsoft Health services, including health-related data and data processed from third-party services, is shared with Cortana. Cortana's capabilities allow you to perform queries and set reminders with your voice, if Cortana is enabled on your device. To learn more about how Cortana manages your data, see the Cortana section of this privacy statement.

HealthVault

HealthVault is a personal health platform that lets you gather, edit, store, and share health data online. With HealthVault, you can control your own health records. You can also choose to share your health data with family, caregivers, health care professionals, mobile applications, health-related devices, and online tools. For more information about HealthVault, visit the HealthVault Help page.

Signing in to HealthVault. To sign in to HealthVault, you can use Microsoft account or third-party authentication services. If you close your Microsoft account or lose your account credentials, you may not be able to access your data. You can use more than one credential with HealthVault to help ensure continued access. Before using a third-party authentication service with HealthVault, we recommend you review the security and privacy commitments offered by the issuer.

HealthVault account and Health records. To create a new HealthVault account, you must provide personal data such as name, date of birth, e-mail address, postal code, and country/region. Depending on which features you use, you may be asked for additional information. A HealthVault account allows you to manage one or more health records, such as the ones you create for yourself and your family members. You can add or remove data to a health record you manage at any time.

In the U.S., HealthVault assigns each health record a unique HealthVault email address. When a message is received at that email address, the message and attachments are automatically added to the HealthVault record, and a notification email is sent to the custodians of that record. The email service in HealthVault uses "Direct," a protocol designed specifically to communicate with health care providers. For that reason, HealthVault email can only be sent and received with providers that use a system that uses the Direct protocol. Custodians can add or disable record email addresses.

Sharing health data. A key value of HealthVault is the ability you have to share your health

data with people and services that can help you meet your health-related goals. By default, you are the custodian of any records you create. Custodians have the highest level of access to a health record. As a custodian, you can share data in a health record with another person by sending an e-mail invitation through HealthVault. You can specify what type of access they have (including custodian access), how long they have access, and whether they can modify the data in the record. When you grant someone access, that person can grant the same level of access to someone else (for example, someone with view-only access can grant another user view-only access). **Because inappropriate granting of access could allow someone to violate your privacy or even revoke your access to your own records, you should be cautious about granting access to your records.**

You can choose to share specific data (or all of the data) in a health record with other services, including participating third-party services you authorize. No service has access to your data through HealthVault unless an authorized user grants it access through HealthVault. HealthVault allows you to control access by accepting or denying requests. For each service granted access, you choose what health information in a specific health record to share and what actions each service may perform on the health information.

A service you authorize for a record will get the full name associated with your HealthVault account, the nickname of the authorized record(s), and your relationship to that record. The service will continue to have access through HealthVault until you revoke the permission. Microsoft can revoke a service's access to HealthVault if it does not meet its privacy commitments to Microsoft. However, except for applying the access permissions you have granted to third-party services, we do not control or monitor third-party services, and their privacy practices will vary.

Reports to U.S. health care providers. In the United States, we enable participating health care providers to obtain reports about whether the information they send to a record in Microsoft Health services is used. This feature supports the "meaningful use" objective of the HITECH Act, which provides incentives for health care providers to send their patients copies of their medical information electronically. Providers that participate can get reports that include a number the provider uses to identify the patient within its system, and whether the user took one of the "qualifying actions" in HealthVault (but no information about which action). "Qualifying action" currently includes activities such as viewing, downloading, or transmitting health information via email. You can turn off reporting for your records.

Access and controls. You can review, edit, or delete your HealthVault account data, or close your HealthVault account at any time. Only custodians can permanently delete an item. When you delete a heath record, it is deleted from all users who had access to it.

When you close your HealthVault account, we delete all records for which you are the sole custodian. If you share custodian access for a record, you can decide whether to delete the record. Microsoft will wait a limited amount of time before permanently deleting your data in order to help avoid accidental or malicious removal of your health data.

HealthVault maintains a full history of each access, change or deletion by users and services, which includes the date, action, and name of the person or service. Custodians of records can examine the history of those records.

Email communications. We will use the email address you provide when you create your HealthVault account to send you an email requesting that you validate your email address, to include in sharing invitations you send through HealthVault, and to send you service notifications, such as email notifications that information is available to add to your HealthVault records.

HealthVault periodically sends newsletters to help keep you informed of the latest improvements. HealthVault will also periodically send you an email summarizing recent account activity. Subject to your contact preferences, we also use your email addresses to send you promotional email. You can unsubscribe from these emails at any time.