



Datenschutzerklärung von Microsoft

Letzte Aktualisierung: Februar 2018 [Neuigkeiten](#)

Der Schutz Ihrer Daten ist uns sehr wichtig. Diese Datenschutzbestimmung erläutert, welche persönlichen Daten Microsoft durch Interaktionen mit Ihnen oder durch unsere Produkte von Ihnen erhebt und wie wir diese Daten verwenden.

Microsoft bietet eine Vielzahl von Produkten an. Diese umfassen Server-Produkte, die verwendet werden, um den Betrieb von Unternehmen weltweit zu unterstützen, Geräte, die Sie in Ihrem Haus verwenden, Software, die von Studenten in der Universität verwenden und Services, die Entwickler zum Erstellen und Hosten von zukünftiger Technologie nutzen. Verweise auf Microsoft-Produkte in dieser Bestimmung beziehen sich auf Microsoft-Dienste, Webseiten, Apps, Software, Server und Geräte von Microsoft.

Bitte lesen Sie die produktspezifischen Informationen in diesen Datenschutzbestimmungen, die zusätzliche Informationen zu einigen Microsoft-Produkten bieten. Diese Datenschutzerklärung gilt für alle Interaktionen von Microsoft mit Ihnen und für die im Folgenden aufgeführten sowie für andere Microsoft-Produkte, die diese Datenschutzerklärung enthalten.

Von uns erhobene personalisierte Daten

Microsoft erhebt Daten, um effektiv arbeiten und Ihnen die besten Erfahrungen mit unseren Produkten anbieten zu können. Sie stellen einige dieser Daten direkt bereit, beispielsweise wenn Sie ein Microsoft-Konto erstellen, das Lizenzabkommen Ihres Unternehmens verwalten, eine Suchanfrage bei Bing einreichen, an einem Microsoft-Event teilnehmen, einen Sprachbefehl an Cortana erteilen, ein Dokument auf Microsoft OneDrive hochladen, ein MSDN-Abonnement erwerben, Office 365 registrieren oder wenn Sie sich hinsichtlich des Supports an uns wenden. Weitere Daten erhalten wir, indem wir Ihre Interaktion mit unseren Produkten aufzeichnen, wenn Sie beispielsweise Technologien wie [Cookies](#) nutzen und wir Fehlermeldungen oder Nutzungsdaten von der Software erhalten, die auf Ihrem Gerät installiert ist.

Wir erhalten ebenfalls Daten von Drittanbietern. Wir schützen die Daten von Drittanbietern gemäß den in den vorliegenden Bestimmungen beschriebenen Richtlinien und alle anderen Einschränkungen der Quellen, aus der die Daten stammen. Diese Drittanbieter-Quellen können sich mit der Zeit ändern und enthielten bisher:

- Daten-Broker, von denen wir demografische Daten erwerben, um die erhobenen Daten zu ergänzen.

- Soziale Netzwerke, wenn Sie einem Microsoft-Produkt den Zugriff auf Ihre Daten auf einem oder mehreren Netzwerken erteilen.
- Dienstanbieter, die uns dabei helfen, einen Standort auf der Basis Ihrer IP-Adresse zu bestimmen, um bestimmte Produkte an Ihren Standort anzupassen.
- Partner, für die wir Co-Branding-Dienste und gemeinsame Marketing-Aktivitäten bereitstellen und
- allgemein verfügbare Datenquellen wie öffentliche staatliche Datenbanken oder andere Public Domain-Daten.

Sie können bestimmen, welche Daten wir erheben. Wenn Sie aufgefordert werden, persönliche Daten zur Verfügung zu stellen, können Sie dies ablehnen. Wenn Sie sich jedoch dazu entscheiden, keine Daten anzubieten, die für eine Bereitstellung eines Produkts oder einer Funktion erforderlich sind, werden Sie möglicherweise nicht in der Lage sein, das Produkt oder die Funktion zu verwenden.

Die erhobenen Daten sind vom Kontext Ihrer Interaktionen mit Microsoft abhängig, Ihren Präferenzen, einschließlich der Datenschutzeinstellungen und den Produkten und Features, die Sie verwenden. Die von uns erhobenen Daten können folgendes umfassen:

Name und Kontaktdaten. Wir erfassen Ihren Vor- und Nachnamen, Ihre E-Mail-Adresse, Postanschrift, Telefonnummer und andere ähnliche Kontaktdaten.

Anmeldeinformationen. Wir erfassen Kennwörter, Kennworthinweise und ähnliche Sicherheitsinformationen, die zur Authentifizierung und für den Kontozugriff verwendet werden.

Demografische Daten. Wir erheben Daten über Sie, z. B. Ihr Alter, Geschlecht, Land und Ihre bevorzugte Sprache.

Zahlungsdaten. Wir erheben Daten, die für die Verarbeitung Ihrer Zahlung bei Einkäufen wichtig sind, wie beispielsweise Ihre Zahlungsmittelnummer (z. B. die Kreditkartennummer) und den mit dem Zahlungsmittel verbundenen Sicherheitscode.

Geräte- und Nutzungsdaten. Wir erfassen Daten über Ihr Gerät und darüber, wie Sie und Ihr Gerät mit Microsoft und unseren Produkten interagieren. Wir erfassen beispielsweise:

- *Produktnutzungsdaten.* Wir erheben Daten über die Funktionen, die Sie verwenden, die Artikel, die Sie kaufen, und die von Ihnen besuchten Webseiten. Zu diesen Daten gehören die Texte Ihrer Sprach- und Suchabfragen oder Befehle für Bing, Cortana und unsere Chat-Bots. Dies umfasst auch die Einstellungen, die Sie auswählen und die am häufigsten von Ihnen verwendeten Softwarekonfigurationen.
- *Geräte-, Verbindungs- und Konfigurationsdaten.* Wir erfassen Daten über Ihr Gerät und das Netzwerk, das Sie für die Verbindung mit unseren Diensten verwenden. Dazu gehören Daten über die Betriebssysteme und andere auf Ihrem Gerät installierte Software, einschließlich dem Product Key. Erfasst werden ebenfalls IP-Adressen, Geräteidentifikator (wie z. B. die IMEI-Nummer für Telefone), Regions- und Spracheinstellungen.

- *Fehlerberichte und Leistungsdaten.* Wir erfassen Daten über die Leistung der Produkte und alle Probleme, die dabei auftreten. Diese Informationen helfen uns beim Diagnostizieren und Beheben von Problemen in den von Ihnen verwendeten Produkten, sowie bei der Verbesserung dieser Produkte. Fehlerberichte (auch „Absturzbilder“ genannt) können je nach Produkt und Einstellungen Daten wie Typ oder Schweregrad des Problems enthalten, sowie Details der im Zusammenhang mit dem Fehler verwendeten Software oder Hardware, Inhalt der beim Auftreten des Fehlers verwendeten Dateien und Daten über andere, auf Ihrem Gerät enthaltene Software.
- *Problembehandlung und Hilfedaten.* Wenn Sie sich für eine Problembehandlung und Hilfe an Microsoft wenden, erfassen wir Daten über Sie und Ihre Hardware, Software und andere Details im Zusammenhang mit der Anfrage. Solche Daten enthalten Kontakte oder Authentifizierungsdaten, den Inhalt Ihrer Chats oder Ihre Kommunikation mit Microsoft, Informationen über den Zustand des Computers und der Anwendung beim Auftreten und bei der Diagnose des Problems, zudem System- und Registrierungsdaten über Softwareinstallationen und Hardwarekonfigurationen.

Interessen und Favoriten. Wir erfassen Daten über Ihre Interessen und Favoriten wie z. B. die Mannschaften, denen Sie in einer Sport-App folgen, Ihre bevorzugte Programmiersprache, die Aktien, die Sie in einer Finanzierungs-App verfolgen oder die Lieblingsstädte, die Sie auf einer Wetter-App hinzufügen. Zusätzlich zu den von Ihnen explizit zur Verfügung gestellten Daten können Ihre Interessen und Favoriten auch von weiteren, von uns erfassten Daten entnommen oder abgeleitet werden.

Kontakte und Beziehungen. Wenn Sie ein Microsoft-Produkt wie beispielsweise Outlook.com verwenden, um Kontakte zu verwalten oder um mit anderen Personen oder Organisationen zu kommunizieren oder zu interagieren, erfassen wir Daten über Ihre Kontakte und Beziehungen, z. B. Visual Studio Team Services.

Positionsdaten. Bei Produkten mit Ortungsdienstfunktionen erheben wir Daten über Ihre Position, die entweder genau oder ungenau sein können. Genaue Positionsdaten können Global Navigation Satellite System (GNSS)-Daten sein (wie GPS), sowie Daten, die in der Nähe befindliche Mobilfunkmasten und WLAN-Hotspots identifizieren. Wir erfassen diese Daten, sobald Sie standortbezogene Produkte und Funktionen aktivieren. Ungenaue Positionsdaten enthalten beispielsweise einen Standort, der von Ihrer IP-Adresse oder Daten abgeleitet wurde. Oder es handelt sich um Daten (wie z. B. eine Stadt oder einen Postleitzahlbereich), die mit geringerer Genauigkeit Aufschluss darüber geben, wo Sie sich aufhalten.

Inhalte. Falls erforderlich, erfassen wir die Inhalte Ihrer Dateien und Mitteilungen, um Ihnen die Nutzung der von Ihnen verwendeten Produkte zu ermöglichen. Wenn Sie beispielsweise eine Datei über Skype an einen anderen Skype-Benutzer übertragen, müssen wir den Inhalt dieser Datei sammeln und ihn für Sie und den anderen Benutzer anzeigen. Wenn Sie eine E-Mail mithilfe von Outlook.com erhalten, müssen wir den Inhalt dieser E-Mail erheben, um Sie in Ihrem Posteingang auszuliefern, diese Ihnen anzuzeigen, Ihnen die Möglichkeit geben, darauf zu antworten, und sie solange zu speichern, bis Sie

entscheiden, sie zu löschen. Andere von uns erfasste Daten bei unseren Kommunikationsdiensten umfassen:

- Betreffzeile und Textkörper einer E-Mail,
- Text oder andere Inhalte einer Sofortnachricht,
- Audio- und Videoaufzeichnung einer Videobotschaft sowie
- die Audioaufzeichnung und Abschrift einer empfangenen SMS oder einer diktierten Textnachricht.

Video. In unseren Microsoft Store-Einzelhandelsgeschäften, unseren anderen Einrichtungen oder bei Veranstaltungen von Microsoft kann Ihr Bild möglicherweise durch unsere Überwachungskameras erfasst werden.

Wenn Sie „Ausgaben“ verwenden, können auch Zahlungsinformationen für die Karte, Belegdaten oder andere Finanztransaktionsdaten erfasst werden, die wir benötigen, um den Dienst bereitzustellen.

Bei der Verwendung von [Onlinedienste für Unternehmen](#), sammelt Microsoft **Kundendaten** (mit Inhalt), **Support-Daten** und **Administratordaten**, wie im Abschnitt unten aufgeführt [Produkte für Unternehmen und Entwickler](#).

Wir sammeln auch Informationen, die Sie uns zur Verfügung stellen, die Inhalte von Meldungen, die Sie uns senden, wie beispielsweise Feedback und Produktbeurteilungen, die Sie schreiben, oder Fragen und Informationen, die Sie unserem Kunden-Support übermitteln. Wenn Sie sich an uns wenden, z. B. für Kundensupport, können Telefongespräche oder Chat-Sitzungen mit unseren Beratern überwacht und aufgezeichnet werden.

Die nachfolgenden produktspezifischen Abschnitte beschreiben die Datenerfassungspraktiken, die für die Verwendung solcher Produkte gelten.

Wie wir personenbezogene Daten nutzen

Microsoft nutzt die erfassten Daten für drei grundlegende Zwecke, die nachfolgend ausführlicher beschrieben werden: (1) für unsere Geschäftstätigkeit und zur Bereitstellung (einschließlich Verbesserung und Personalisierung) der von uns angebotenen Produkte, (2) zum Senden von Mitteilungen, einschließlich Werbenachrichten, und (3) zum Anzeigen von Werbung in einigen Produkten, die durch die Werbung z. B. von MSN und Bing, oder denen von Drittanbietern, unterstützt werden.

Zu diesem Zweck kombinieren wir Daten, die wir erfassen, um Ihnen eine nahtlose, konsistente und personalisierte Erfahrung zu bieten. Beispielsweise kann [Cortana](#) anhand der Lieblingssportteams, die Sie zur Microsoft Sport-App hinzufügen, für Sie interessante Informationen bereitstellen, [Microsoft Store](#) kann anhand der Informationen darüber, wie Sie verschiedene Apps und Dienste nutzen, personalisierte App-Empfehlungen erstellen. Um jedoch die Privatsphäre zu verbessern, haben wir technologische und verfahrensrechtliche Garantien integriert, welche dafür konzipiert sind, bestimmte Datenkombinationen zu verhindern. So speichern wir beispielsweise Daten, die wir

erheben, während Sie unbestätigt (nicht angemeldet) sind, getrennt von Kontoinformationen, durch die Sie direkt identifiziert werden können - wie beispielsweise Ihren Namen, Ihre E-Mail-Adresse oder Telefonnummer.

Bereitstellung und Verbesserung unserer Produkte. Wir verwenden Daten, um angebotene Produkte zur Verfügung zu stellen und zu verbessern, und um notwendige Geschäftsvorgänge auszuführen. Dies gilt für den Betrieb der Produkte, die Erhaltung und Verbesserung der Leistung dieser Produkte, einschließlich der Entwicklung neuer Funktionen, der Forschung und der Kundenbetreuung. Im Folgenden finden Sie Beispiele für eine solche Verwendungen:

- **Bereitstellung der Produkte.** Wir verwenden Daten, um Ihre Transaktionen mit uns durchzuführen und Ihnen unsere Produkte anbieten zu können. Häufig enthalten diese Produkte personalisierte Funktionen und Empfehlungen, die Ihre Produktivität und Ihren Genuss erhöhen, und Ihre Erfahrungen mit den Produkten automatisch auf Grundlage der von uns gesammelten Daten über Ihrer Aktivitäten, Interessen und Ihrem Standort anpassen.
- **Kundendienst.** Wir verwenden Daten, um Probleme mit Produkten zu diagnostizieren, Geräte von Kunden zu reparieren und andere Kundenbetreuungs- und -Support-Dienste anzubieten.
- **Produktaktivierung.** Wir verwenden Daten – wie beispielsweise Gerätetyp und Art der verwendeten App, Position und eindeutige Geräte-, App-, Netzwerk- und Abonnement-Identifikatoren – um Software und Geräte zu aktivieren, die eine Aktivierung erfordern.
- **Verbesserung der Produkte.** Wir verwenden Daten, um unsere Produkte durch das Hinzufügen neuer Features oder Fähigkeiten ständig zu verbessern. Wir verwenden beispielsweise Fehlerberichte, um die Sicherheitsfunktionen zu verbessern, Suchanfragen und -klicks in Bing, die die Relevanz der Suchergebnisse verbessern, Nutzungsdaten, die uns bei der Priorisierung neuer Funktionen helfen oder Audio-Aufnahmen von Spracheingabefeatures, die die Spracherkennungsgenauigkeit verbessern.
- **Sicherheits- und Konfliktlösung.** Wir verwenden Daten, um die Sicherheit unserer Produkte und unserer Kunden zu schützen, Betrug aufzudecken und zu verhindern, die Gültigkeit von Software-Lizenzen zu bestätigen, Streitfälle zu schlichten und Vereinbarungen durchzusetzen. Unsere Sicherheitsfunktionen und -produkte können die Funktion von Schadsoftware unterbrechen und Benutzer darüber benachrichtigen, falls Schadsoftware auf deren Geräten gefunden wurde. Beispielsweise scannen unsere Mitteilungs- und Datei-Synchronisierungsprodukte wie Outlook oder OneDrive systematisch Inhalte auf automatisierte Weise, um mutmaßlichen Spam, Viren, missbräuchliche Handlungen oder URLs, die als Betrug gekennzeichnet wurden sowie Phishing- oder Malware-Links zu identifizieren. Wir können die Versendung einer Mitteilung blockieren oder deren Inhalt entfernen, wenn es gegen unsere AGB verstößt.
- **Geschäftstätigkeit.** Wir nutzen Daten zur Entwicklung aggregierter Analysen und Business-Intelligenz, die es uns ermöglichen, unser Geschäft zu betreiben, dieses zu

schützen, informierte Entscheidungen darüber zu treffen und Berichte über deren Leistungsfähigkeit zu erstellen.

Kommunikation. Wir verwenden erfasste Daten, um unsere Kommunikation mit Ihnen zu personalisieren und bereitzustellen. Zum Beispiel kontaktieren wir Sie möglicherweise per Telefon oder E-Mail oder durch andere Methoden, um Sie darüber zu informieren, wann ein Abonnement endet, Ihren Lizenzvertrag zu besprechen oder Sie wissen zu lassen, wann Sicherheitsupdates verfügbar sind, oder Sie daran zu erinnern, welche Artikel sich noch in Ihrem Einkaufswagen befinden. Eventuell halten wir Sie über eine Dienste- oder Reparaturanfrage auf dem Laufenden oder laden Sie zur Teilnahme an einer Umfrage ein oder teilen Ihnen mit, dass Sie eine Maßnahme treffen müssen, um Ihr Konto aktiv zu halten. Darüber hinaus können Sie sich für E-Mail-Abonnements registrieren und wählen, ob Sie Werbemitteilungen von Microsoft per E-Mail, SMS, physischer Post und Handy erhalten möchten. Für Informationen über das Verwalten von Kontaktdaten, E-Mail-Abonnements und von Werbemitteilungen besuchen Sie bitte den Abschnitt [Zugriff und Steuerung](#) dieser Datenschutzbestimmungen.

Werbung. Microsoft verwendet keine Ihrer Inhalte aus E-Mails, Chats, Videoanrufen oder Voicemails oder Ihren Dokumenten, Fotos oder anderen persönlichen Dateien, um damit Werbung zu erzeugen, die auf Sie zielt.

Wir verwenden die durch unsere Interaktionen mit Ihnen in puncto Produkte und Drittanbieter-Web-Eigenschaften gesammelten Daten, um Werbungen anzuzeigen. Zum Beispiel:

- Microsoft verwendet eventuell Ihre Daten, um einige der Anzeigen auszuwählen und anzubieten, die Sie auf Microsoft-Webseiten sehen, wie z. B. Microsoft.com, MSN und Bing.
- Wenn die Werbe-ID in Windows 10 als Teil der Datenschutzeinstellungen aktiviert ist, können Microsoft-Apps auf diese zugreifen und sie verwenden (ähnlich wie Webseiten, die auf eine eindeutige, in einem Cookie gespeicherte Kennung, zugreifen), um Werbungen für diese Apps auszusuchen und anzubieten.
- Wir teilen die Daten, die wir mit Drittanbietern wie Oath, AppNexus oder Facebook (siehe unten), erfassen, damit diese Anbieter Werbeanzeigen in unseren Produkten oder andere Produkte und für ihre oder unsere Webseiten und Apps auswählen und anbieten können.
- Werbetreibende können unsere [Web-Beacons](#) auf ihrer Webseite platzieren, um Microsoft zu erlauben, auf deren Webseiten Informationen wie Aktivitäten, Einkäufe und Besuche zu erfassen. Wir nutzen diese Daten im Auftrag unserer Werbekunden, um deren Werbung zielgerichtet zu orientieren. Außerdem werden Daten direkt an Dienstleister wie Oath, AppNexus oder Facebook weitergegeben, um ihnen die Möglichkeit zu bieten, Dienste im Auftrag von Microsoft zur Verfügung zu stellen oder bei der Auswahl und Bereitstellung von Anzeigen für Werbepartner zu kooperieren.

Die dargestellte Werbung kann auf Daten wie Ihren Interessen und Favoriten, Ihrem aktuellen Standort, Ihren Transaktionen, der Verwendung unserer Produkte, Suchkriterien

oder auf Inhalten basieren, die Sie sich gerade ansehen. Wenn Sie sich beispielsweise Inhalte auf MSN zum Thema Auto anschauen, zeigen wir Autowerbungen an. Wenn Sie „Pizzerien in Seattle“ auf Bing suchen, sehen Sie Werbungen in Ihren Suchergebnissen für Restaurants in Seattle.

Weitere Werbung basiert auf andere Informationen, die wir im Laufe der Zeit aus demografischen Daten, Positionsdaten, Suchabfragen, Interessen, Hobbys und Favoriten, Nutzungsdaten von unseren eigenen Produkten und Webseiten sowie von den Webseiten und Apps unserer Partner über Sie erfahren haben. Diese Art von Werbung wird in diesen Bestimmungen als „interessenbezogene Werbung“ klassifiziert. Wenn Sie z. B. Spielinhalte auf xbox.com anzeigen, werden Angebote für Spiele auf MSN angezeigt. Um interessenbezogene Werbung zu bieten, speichern wir, sobald Ihr Browser mit unseren Webseiten interagiert, Cookies auf Ihrem Gerät, die von uns erfasste Informationen (beispielsweise Ihre IP-Adresse) enthalten. Wenn Sie den Empfang interessenbezogener Werbung ablehnen, werden die diesen Cookies zugeordneten Daten nicht verwendet.

Weitere Details zur werbebezogenen Verwendungen von Daten umfassen:

- **In der Werbebranche anerkannte und bewährte Vorgehensweisen und Verpflichtungen.** Microsoft ist Mitglied der [Network-Advertising-Initiative](#) (NAI) und hält die Verhaltensregeln der NAI ein. Wir halten uns zudem an die folgenden Selbstregulierungsprogramme:
 - In den USA: [Digital Advertising Alliance \(DAA\)](#)
 - In Europa: [European Interactive Digital Advertising Alliance \(EDAA\)](#)
 - In Kanada: [Ad Choices: Digital Advertising Alliance of Canada \(DAAC\)](#) / [Choix de Pub: l'Alliance de la publicité numérique du Canada \(DAAC\)](#)
- **Kinder und Werbung.** Wir versenden keine interessenbezogene Werbung an Kinder, deren Geburtsdatum in ihrem Microsoft-Konto diese als unter 13 Jahre alt identifiziert.
- **Datenvorhaltung.** Die Daten aus interessenbezogener Werbung werden von uns nicht länger als 13 Monate vorgehalten, es sei denn, dass wir Ihr Einverständnis bekommen, die Daten länger vorzuhalten.
- **Datenfreigabe.** In einigen Fällen teilen wir Berichte mit den Werbungtreibenden über solche Daten, die wir auf ihren Webseiten oder von ihrer Werbung erfasst haben.
- **Daten, die von anderen Unternehmen erfasst werden.** Werbetreibende integrieren mitunter eigene [Web-Beacons](#) (bzw. die anderer Werbepartner) in die von uns angezeigte Werbung, um eigene [Cookie-](#) zu platzieren. Zusätzlich werden Microsoft-Partner mittels Drittanbieter-Ad-Unternehmen dabei helfen, einige unserer Werbe-Dienste anzubieten und wir erlauben auch anderen Drittanbieter-Ad-Unternehmen, Werbung auf unseren Seiten zu platzieren. Diese Drittanbieter können auch Cookies auf Ihrem Computer platzieren und Informationen über Ihre Onlineaktivitäten auf Webseiten oder Onlinediensten erheben. Dazu gehören momentan u. a. folgende Unternehmen: [A9](#), [AppNexus](#), [Criteo](#), [Facebook](#), [MediaMath](#), [nugg.adAG](#), [Oath](#), [Rocket Fuel](#), [Yahoo!](#). Sie erhalten weitere Informationen über die Praktiken jedes einzelnen Unternehmens, einschließlich der angebotenen Optionen, indem Sie auf den Firmennamen oben klicken. Viele von

ihnen sind Mitglieder der [NAI](#) oder der [DAA](#), die jeweils eine einfache Methode zur Ablehnung von Zielgruppenwerbung von Seiten der teilnehmenden Unternehmen anbieten.

Gründe, Warum Wir Persönliche Daten Teilen

Wir teilen Ihre persönlichen Daten mit Ihrer Zustimmung oder nach Bedarf, um eine Transaktion abzuschließen oder ein Produkt anbieten zu können, das Sie angefordert oder autorisiert haben. Zum Beispiel teilen wir Ihre Inhalte mit Drittanbietern, wenn Sie uns anweisen, dies so zu tun, wie zum Beispiel, wenn Sie eine E-Mail an einen Freund, Fotos und Dokumente auf OneDrive oder Konten mit einem anderen Dienst verknüpfen. Wenn Sie Zahlungsdaten liefern, um einen Kauf zu tätigen, werden wir die Zahlungsdaten mit Banken und anderen Unternehmen teilen, die den Zahlungsverkehr bearbeiten oder andere Finanzdienstleistungen anbieten sowie zur Betrugsprävention und für die Kreditrisikominderung.

Darüber hinaus teilen wir personenbezogene Daten mit Microsoft-kontrollierten verbundenen Unternehmen und Tochtergesellschaften. Wir teilen auch personenbezogene Daten mit Lieferanten oder Agenten, die in unserem Namen für die hier beschriebenen Zwecke tätig sind. Zum Beispiel benötigen Unternehmen, die wir beauftragt haben, um den Kundendienst zu unterstützen oder um zu helfen, die Sicherung unserer Systeme und Dienstleistungen zu schützen und möglicherweise Dienstleister, die Zugang zu personenbezogenen Daten haben müssen, um diese Funktionen zu ermöglichen. In solchen Fällen müssen diese Unternehmen unsere Datenschutz- und Sicherheitsbestimmungen einhalten und dürfen die von uns erhaltenen, personenbezogenen Daten nicht für andere Zwecke verwenden. Des Weiteren kann Microsoft persönliche Daten im Rahmen seines unternehmerischen Handelns wie z. B. einer Fusion oder der Veräußerung von Vermögenswerten weitergeben.

Schließlich greifen wir auf persönliche Daten inklusive Ihrer privaten Inhalte (wie die Inhalte Ihrer E-Mails in Outlook.com oder Dateien in privaten Ordnern auf OneDrive) zu, übertragen sie, legen sie offen und bewahren sie auf, wenn wir in gutem Glauben annehmen, dass dies notwendig ist, um:

1. geltende Gesetze einzuhalten oder auf gerichtliche Verfahren zu antworten, einschließlich denen von Strafverfolgungsbehörden oder anderen staatlichen Stellen;
2. unsere Kunden zu schützen, zum Beispiel, um Spam oder Versuche, Nutzer unserer Produkte zu betrügen oder zu helfen, den Verlust von Leben oder schweren Verletzungen von Personen zu verhindern;
3. dauerhaft die Sicherheit unserer Produkte zu gewährleisten, einschließlich einen Angriff auf unsere Computersysteme oder Netzwerke zu verhindern oder zu stoppen; oder
4. die Rechte oder das Eigentum von Microsoft, einschließlich der Durchsetzung der Bedingungen für die Nutzung der Dienste zu schützen. Wenn wir jedoch Informationen erhalten, dass jemand unsere Dienstleistungen für den Handel mit gestohlenem geistigem oder physischem Eigentum von Microsoft benutzt, werden

wir Privatinhalte eines Kunden nicht selbst inspizieren, sondern die Angelegenheit an die Strafverfolgungsbehörden weiterleiten.

Weitere Informationen zu den Daten, die wir auf Anfrage von Strafverfolgungs- und anderen Regierungsbehörden offenlegen, finden Sie in unserem Law Enforcement Transparency Report (Bericht zur Transparenz des Gesetzesvollzugs) unter microsoft.com/about/corporatecitizenship/en-us/reporting/transparency.

Beachten Sie, dass einige unserer Produkte Links zu Produkten von Drittanbietern enthalten, deren Datenschutzrichtlinien sich von denen von Microsoft unterscheiden. Wenn Sie persönliche Daten an eines dieser Produkte übermitteln, unterliegen Ihre Daten den zugehörigen Datenschutzrichtlinien.

Wie das Zugreifen und Steuern Ihrer persönlichen Daten funktioniert

Sie können Ihre persönlichen Daten für viele Microsoft-Produkte Online ansehen, bearbeiten und löschen. Sie können auch darüber entscheiden, wie Microsoft Ihre Daten erfasst und nutzt. Wie Sie auf Ihre Daten zugreifen oder diese steuern können hängt davon ab, welche Produkte Sie verwenden. Zum Beispiel:

- **Microsoft-Datenschutz-Dashboard.** Hier können Sie Aktivitätsdaten auf mehreren Microsoft-Diensten des Microsoft-Datenschutz-Dashboards anzeigen und kontrollieren: account.microsoft.com/privacy. Von hier aus können Sie Browser-, Such- und Positionsdaten, die mit Ihrem Microsoft-Konto verknüpft sind anzeigen und löschen. Sie können ebenfalls Daten in Ihrem Cortana-Notizbuch und im Microsoft Health-Dienste verwalten.
- **Volume Licensing Service Center (VLSC).** Von [Hier](#) erhalten Sie einen einfachen Zugriff auf alle Ihre Lizenzinformationen an einem Ort.
- **Microsoft-Konto.** Wenn Sie die Profil- und Zahlungsinformationen auf Ihrer [Microsoft-Konto](#) aufrufen, bearbeiten oder löschen, Ihr Kennwort ändern, Sicherheitsinformationen hinzufügen oder Ihr Konto schließen möchten, rufen Sie account.microsoft.com auf. Von hier aus können Sie auch auf die Steuerung anderer Microsoft-Produkte zugreifen.
- **Skype.** Wenn Sie die Profil- und Zahlungsinformationen in Ihrem Skype-Konto aufrufen, bearbeiten, löschen oder Ihr Kennwort ändern möchten, können Sie sich bei Ihrem Konto unter login.skype.com/login anmelden.
- **Xbox.** Wenn Sie Xbox Live oder Xbox.com nutzen, können Ihre persönlichen Daten, einschließlich Abrechnungs- und Kontoinformationen sowie Einstellungen für Datenschutz, Onlinesicherheit und Datenfreigabe, über [Meine Xbox](#) auf der Xbox-Konsole oder auf der Webseite Xbox.com aufgerufen oder bearbeitet werden.
- **Microsoft Store.** Sie können auf Ihr Microsoft Store-Profil und Ihre Kontoinformationen zugreifen, indem Sie www.microsoftstore.com/ aufrufen und auf „Konto anzeigen“ oder „Bestellverlauf“ klicken
- **Microsoft.com.** Sie können auf Ihr Profil auf microsoft.com im [Microsoft.com Profil-Zentrum](#) zugreifen und es aktualisieren.
- Wenn Sie über ein öffentliches MSDN-Profil verfügen, können Sie dieses unter connect.microsoft.com/profile.aspx aufrufen und bearbeiten.

Wenn Sie nicht über die obigen Links auf bestimmte persönliche Daten zugreifen können, die von Microsoft erfasst werden, bzw. nicht direkt über die Microsoft-Produkte, die Sie verwenden, auf persönliche Daten zugreifen können, ist es Ihnen jederzeit möglich, Microsoft über das [Webformular](#) zu kontaktieren. Wir werden innerhalb von 30 Tagen auf Anfragen reagieren, um Ihre persönlichen Daten einzusehen oder zu löschen.

Ihre Kommunikationspräferenzen

Sie haben die Wahl, ob Sie Werbemitteilungen von Microsoft per E-Mail, SMS, physischer Post oder Telefon erhalten möchten. Wenn Sie eine Werbe-Email oder SMS-Nachricht von uns erhalten und diese aber in Zukunft nicht mehr erhalten möchten, befolgen Sie einfach die Anweisungen in dieser Nachricht. Wenn Sie den [Microsoft-Konto](#) von Microsoft mit Ihrer persönlichen [Kommunikationsberechtigungen](#) aufrufen und sich dort anmelden, stehen Ihnen Auswahlmöglichkeiten über den Empfang von Werbe-E-Mails, Telefonanrufen und Postsendungen zur Verfügung. Hier können Sie Kontaktinformationen aktualisieren, Ihre Kontaktpräferenzen bei Microsoft verwalten, Abonnements stornieren und auswählen, ob Sie Ihre Kontaktinformationen mit Microsoft-Partnern teilen möchten. Wenn Sie kein persönliches Microsoft-Konto haben, können Sie die Präferenzen im Hinblick auf Ihren E-Mail-Kontakt mit Microsoft auch über dieses [Webformular](#) verwalten. Diese Auswahlmöglichkeiten gelten nicht für obligatorische Dienstkommunikationen, die Teil gewisser Microsoft-Dienste sind oder für Umfragen oder andere informative Kommunikationen, die ihre eigenen Kündigungsverfahren aufweisen.

Ihre Werbeoptionen

Sie können den Erhalt interessenbasierter Werbung von Microsoft ablehnen, indem Sie folgende Seite besuchen: [Opt-Out-Seite](#). Nach der Ablehnung wird Ihre Auswahl in einem für Ihren Computer und den verwendeten Webbrowser spezifischen [Cookie](#) gespeichert. Dieses Opt-Out-Cookie hat eine Gültigkeit von fünf Jahren. Falls Sie Cookies auf Ihrem Computer löschen, muss die Ablehnung wiederholt werden.

Sie können Ihre Opt-Out-Wahl auch mit Ihrem persönlichen Microsoft-Konto verknüpfen. Diese gilt dann für jedes Gerät, auf dem Sie dieses Konto verwenden, und bleibt bestehen, bis Sie sich mit einem anderen persönlichen Microsoft-Konto an diesem Gerät anmelden. Wenn Sie Cookies auf Ihrem Gerät löschen, müssen Sie sich erneut anmelden, damit die Einstellung wieder angewendet w.

Für Werbung, die in Apps unter Windows angezeigt wird, können Sie die mit Ihrem persönlichen Microsoft-Konto verknüpfte Ablehnung verwenden. Sie können auch die [Werbe-ID](#) in den Windows-Einstellungen deaktivieren, um interessenbezogene Werbung abzulehnen.

Da die für die interessenbezogene Werbung verwendeten Daten auch für andere Zwecke benötigt werden (einschließlich der Bereitstellung unserer Produkte, Analysen und der Betrugserkennung), wird durch ein Abmelden der interessenbezogenen Werbung das Erheben dieser Daten nicht beendet. Es bedeutet auch nicht, dass Sie keine oder weniger Werbung sehen. Wenn Sie ablehnen, werden die Anzeigen, die Sie erhalten, jedoch nicht mehr interessenbezogen sein und sie sind für Sie möglicherweise weniger von Interesse.

Sie können den Erhalt interessensbasierter Werbung von Drittanbietern, mit denen wir eine Partnerschaft haben, ablehnen, indem Sie folgende Seite besuchen: (siehe oben).

Browserbasierte Steuerungen

- **Cookie-Steuerelemente.** Relevante browserbasierte Cookie-Steuerelemente werden im Abschnitt [Cookies](#) dieser Datenschutzerklärung beschrieben.
- **Tracking-Schutz.** Internet Explorer (Versionen 9 und höher) verfügt über ein Feature namens Tracking-Schutz, die Inhalte von Drittanbietern einschließlich Cookies von allen Webseiten blockiert, die in einer von Ihnen hinzugefügten Tracking-Schutzliste enthalten sind. Durch eine Begrenzung der Aufrufe an diese Webseiten werden die Informationen beschränkt, die diese Drittanbieter-Webseiten über Sie sammeln können.
- **Browserkontrollen für „Do Not Track (nicht verfolgen)“.** Einige Browser haben die „Do Not Track“ (DNT)-Features eingearbeitet, die ein Signal an die von Ihnen besuchten Webseiten senden kann, das darauf hinweist, dass Sie nicht nachverfolgt werden möchten. Da es noch keine gemeinsame Verständigung darüber gibt, wie das DNT-Signal interpretiert werden soll, reagieren Microsoft-Dienste momentan nicht auf Browser-DNT-Signale. Wir werden weiterhin mit der Onlinebranche zusammenarbeiten, um eine allgemeine Übereinkunft der DNT-Signalen zu definieren. In der Zwischenzeit können Sie die Bandbreite anderer Werkzeuge benutzen, die wir zur Verfügung stellen, um die Datenerfassung und die Nutzung zu steuern, einschließlich der oben beschriebenen Möglichkeit, sich vom Erhalt interessenbezogener Werbung von Microsoft abzumelden.

Cookies und ähnliche Technologien

Microsoft verwendet Cookies (kleine, auf dem Gerät platzierte Textdateien) und ähnliche Technologien, um unsere Webseiten- und Onlinedienste anzubieten und beim Erheben von Daten zu helfen. Der Text in einem Cookie besteht oft aus einer Reihe von Zahlen und Buchstaben, die Ihren Computer eindeutig identifizieren. Es kann jedoch auch weitere Informationen enthalten. Microsoft-Apps verwenden zusätzliche Erkennungsmöglichkeiten wie die [Werbe-ID](#) in Windows für ähnliche Zwecke, und viele unserer Webseiten und Apps enthalten auch Web-Beacons oder ähnliche Technologien, wie nachfolgend beschrieben.

Unsere Verwendung von Cookies und Vergleichbaren Technologien

Je nach Produkt verwendet Microsoft Cookies und ähnliche Technologien für verschiedene Zwecke, darunter:

- **Speichern Ihrer Präferenzen und Einstellungen.** Einstellungen, die es unseren Produkten ermöglichen, einwandfrei zu funktionieren oder die Ihre Präferenzen beibehalten, können im Laufe der Zeit auf Ihrem Gerät gespeichert werden. Wenn Sie beispielsweise auf einer Microsoft-Seite Ihre Stadt oder Ihre PLZ eingeben, um lokale Nachrichten oder Wetterinformationen über eine Microsoft-Webseite zu erhalten, speichern wir diese Angaben möglicherweise in einem Cookie, um Ihnen beim erneuten Aufrufen dieser Seite die relevanten lokalen Informationen

anzuzeigen. Auch speichern ebenfalls bevorzugte Einstellungen, wie Sprache, Browser und Multimedia-Player-Einstellungen, damit diese nicht jedes Mal zurückgesetzt werden müssen, wenn Sie zur Webseite zurückkehren. Sollten Sie sich von interessenbezogener Werbung abmelden, dann speichern wir mithilfe eines Cookies Ihre Abmeldungspräferenz auf Ihrem Gerät.

- **Anmeldung und Authentifizierung.** Sobald Sie sich mit Ihrem persönlichen [Microsoft-Konto](#) bei einer Webseite anmelden, wird eine eindeutige ID-Nummer sowie die Uhrzeit Ihrer Anmeldung in einem verschlüsselten Cookie auf Ihrem Gerät gespeichert. Dieses Cookie ermöglicht es Ihnen, verschiedene Seiten innerhalb der Webseite aufzurufen, ohne sich auf jeder Seite erneut anmelden zu müssen. Sie können ebenfalls Ihre Anmeldeinformationen speichern, damit Sie sich nicht jedes Mal anmelden müssen, wenn Sie zur Webseite zurückkehren.
- **Sicherheit.** Wir verwenden Cookies, um Betrug und Missbrauch auf unseren Webseiten und Diensten zu erkennen.
- **Speichern Ihrer auf einer Webseite angegebenen Informationen.** Wenn Sie Informationen bereitstellen oder Produkte in den Einkaufswagen beim Einkaufen auf der Microsoft-Webseiten hinzufügen, speichern wir die Daten über die Produkte und Informationen, die Sie hinzugefügt haben in einem Cookie.
- **Soziale Medien.** Einige unserer Webseiten enthalten Social-Media-Cookies, einschließlich Cookies, die den auf dem Social-Media-Dienst angemeldeten Benutzern die Freigabe des Inhalts über diesen Dienst ermöglichen.
- **Feedback.** Microsoft verwendet Cookies, damit Sie Feedback auf einer Webseite bereitstellen können.
- **Interessenbezogene Werbung.** Microsoft-Advertising setzt Cookies ein, um die Daten Ihrer Onlineaktivität zu erfassen und um Ihre Interessen zu identifizieren, sodass wir Ihnen solche Werbung anzeigen können, die für Sie relevant ist. Sie können den Empfang interessenbezogener Werbung von Microsoft ablehnen, wie im Abschnitt [Zugriff und Steuerung](#) dieser Datenschutzbestimmungen beschrieben.
- **Anzeigen von Werbung.** Microsoft verwendet Cookies, um aufzuzeichnen, wie viele Besucher auf eine Anzeige geklickt haben und welche Werbungen Sie sich angesehen haben, damit nicht dieselbe Werbung wiederholt angezeigt wird.
- **Analyse.** Um unsere Produkte anbieten zu können, verwenden wir Cookies und andere Erkennungsmöglichkeiten, die Nutzungs- und Leistungsdaten erheben. Wir benutzen beispielsweise Cookies, um die Zahl der individuellen Besucher einer Webseite oder eines Dienstes zu ermitteln oder um andere Statistiken im Hinblick auf den Betrieb unserer Produkte zu erheben. Dazu zählen Cookies von Microsoft und von Drittanbietern für Analysen
- **Leistung.** Microsoft verwendet Cookies für den Lastenausgleich und um sicherzustellen, dass Webseiten weiterhin optimal ausgeführt werden.

Einige der Cookies, die wir normalerweise benutzen, sind im Folgenden aufgeführt. Diese Liste ist nicht vollständig, sondern soll die Hauptgründe verdeutlichen, wieso wir üblicherweise Cookies einsetzen. Wenn Sie eine unserer Webseiten besuchen, setzen wir möglicherweise folgende Cookies ein:

- **MUID, MC1 und MSFPC** – Identifizieren Web-Browser, die Microsoft-Webseiten besuchen. Diese Cookies werden für Werbung, Seitenanalyse und andere Betriebszwecke benutzt.
- **ANON** - Enthält die ANID, die eine eindeutige Kennung darstellt, welche von Ihrem Microsoft-Konto abgeleitet wurde und für Werbung, Personalisierung und betriebliche Zwecke verwendet wird. Diese wird auch benutzt, um Ihre Auswahl für eine Abmeldung von interessenbezogener Werbung von Microsoft zu erhalten, nachdem Sie diese Abmeldung für Ihr Microsoft-Konto vorgenommen haben.
- **CC** - Es enthält den Ländercode, wie es durch Ihre IP-Adresse bestimmt wurde.
- **PPAuth, MSPAuth, MSNRPSAuth, KievRPSAuth** - Hilft dabei Sie zu authentifizieren, sobald Sie sich mit Ihrem Microsoft-Konto anmelden.
- **NAP** - Enthält eine verschlüsselte Version Ihres Lands, PLZ, Alter, Geschlecht, Sprache und Beruf, falls bekannt, basierend auf dem Profil Ihres Microsoft-Kontos.
- **MH** - Erscheint auf Co-Branded-Webseiten, auf denen Microsoft eine Partnerschaft mit einem Werbepartner eingegangen ist. Dieses Cookie identifiziert den Anbieter, sodass die richtige Anzeige ausgewählt wird.
- **MR** – Wird zum Sammeln von Informationen für die Analyse Zwecke verwendet.
- **TOptOut** - Zeichnet Ihre Entscheidung auf, keine interessenbezogenen Anzeigen von Microsoft geliefert zu bekommen.

Zusätzlich zu den Cookies, die Microsoft beim Besuch einer Webseite setzt, können auch Drittanbieter Cookies platzieren, sobald Sie Seiten von Microsoft besuchen. In einigen Fällen geschieht dies, weil wir Dritte damit beauftragt haben, für uns Dienste wie etwa Seiten-Analysen anzubieten. In anderen Fällen geschieht es, weil unsere Seiten Inhalte oder Anzeigen von Dritten enthalten, wie etwa Videos, Nachrichten oder Anzeigen von anderen Anzeigen-Netzwerken. Da Ihr Browser für den Zugriff auf diese Inhalte eine Verbindung mit den Servern dieser Drittanbieter herstellt, können diese auch ihre eigenen Cookies auf Ihrem Gerät platzieren oder lesen und Informationen über Ihre Onlineaktivitäten auf Webseiten oder in Onlinediensten erfassen.

Kontrollieren von Cookies

Die meisten Web-Browser akzeptieren Cookies automatisch, bieten jedoch Steuerungen, die es Ihnen erlauben, diese zu sperren oder zu löschen. Beispielsweise können Sie in Microsoft Edge Cookies blockieren oder löschen, indem Sie auf **Einstellungen & Datenschutz & Cookies** klicken. Anweisungen zum Blockieren oder Löschen von Cookies in anderen Browsern finden Sie in der zugehörigen Dokumentation zu Datenschutz und Hilfe.

Bestimmte Funktionen von Microsoft-Produkten basieren auf Cookies. Bitte beachten Sie, dass, falls Sie sich dazu entscheiden, Cookies zu blockieren, Sie möglicherweise nicht in der Lage sind sich anzumelden oder diese Funktionen zu verwenden und Einstellungen, die auf Cookies basieren, verloren gehen können. Wenn Sie die Cookies löschen, werden Einstellungen, einschließlich Werbeeinstellungen, die von diesen Cookies gesteuert werden gelöscht und müssen möglicherweise wiederhergestellt werden.

Zusätzliche Datenschutzsteuerelemente, die sich auf Cookies auswirken können, einschließlich des Tracking-Schutz-Features von Microsoft-Browsern, werden im Abschnitt [Zugriff und Steuerung](#) dieser Datenschutzerklärung beschrieben.

Wofür wir Web-Beacons und Analysedienste verwenden

Microsoft-Webseiten enthalten möglicherweise elektronische Bilder, die als Web-Beacons (Auch Einpixel-Gifs genannt) dabei helfen, Cookies zu setzen, um die Anzahl der Besucher dieser Webseiten zu ermitteln und Co-Branding-Produkte bereitzustellen. Wir verwenden Web-Beacons möglicherweise in unseren E-Mail-Werbepublikationen oder in Newslettern, um zu ermitteln, ob die Nachrichten von Ihnen geöffnet werden und Sie darauf reagieren.

Neben der Platzierung von Web Beacons auf unseren eigenen Webseiten, kooperieren wir manchmal mit anderen Unternehmen, indem wir unsere Web Beacons auf deren Webseiten oder in deren Werbung platzieren. Dies hilft uns bei der Entwicklung von Statistiken, wie häufig Sie eine Anzeige auf einer Microsoft-Webseite für einen Kauf anklicken oder zu einer weiteren Aktivität auf der Webseite des Inserenten führte.

Schließlich enthalten Microsoft-Produkte häufig Web Beacons oder ähnliche Technologien von Drittanbietern für Analysen, die uns dabei helfen, zusammengefasste Statistiken über die Wirksamkeit unserer Werbekampagnen oder anderen Operationen zu kompilieren. Diese Technologien ermöglichen den Anbietern von Analysen, ihre eigenen Cookies oder andere Kennungen auf Ihrem Gerät zu platzieren oder zu lesen, durch die sie Informationen über Ihre Onlineaktivitäten quer durch alle Apps, Webseiten oder andere Produkte erheben können. Allerdings verbieten wir den Anbietern von Analysen, die Web Beacons auf unseren Seiten zu verwenden, um Informationen zu erheben oder darauf zuzugreifen, durch die Sie direkt identifiziert werden können (wie Name oder E-Mail-Adresse). Sie können sich von der Datenerhebung oder der Verwendung von einigen dieser Analyseanbieter abmelden, indem Sie auf die folgenden Links klicken:

- Anpassen: www.adjust.com/opt-out
- AppsFlyer: www.appsflyer.com/optout
- Clicktale: www.clicktale.net/disable.html
- Flurry Analytics: <https://aim.yahoo.com/aim/us/en/optout/>
- Google Analytics: tools.google.com/dlpage/gaoptout (erfordert die Installation eines Browser-Add-Ons)
- Kissmetrics: kissmetrics.com/user-privacy
- Mixpanel: mixpanel.com/optout
- Nielsen: www.nielsen-online.com/corp.jsp?section=leg_prs&nav=1#Optoutchoices
- Omniture (Adobe): www.d1.sc.omtrdc.net/optout.html
- Visible Measures: www.visiblemeasures.com/viewer-settings-opt-out
- WebTrends: ondemand.webtrends.com/support/optout.asp

Weitere ähnliche Technologien

Zusätzlich zu den standardmäßigen Cookies und Web Beacons können unsere Produkte auch weitere, ähnliche Technologien benutzen, um Dateien auf Ihrem Computer zu speichern und zu lesen. Dies geschieht üblicherweise, um Ihre Präferenzen zu speichern

oder die Geschwindigkeit und die Leistung zu verbessern, indem bestimmte Dateien lokal gespeichert werden. Wie auch bei Standard-Cookies können diese Technologien aber auch dafür benutzt werden, eine eindeutige Kennung auf Ihrem Computer zu speichern, die dazu verwendet werden kann, Ihr Verhalten nachzuverfolgen. Zu diesen Technologien gehören lokal freigegebene Objekte (oder „Flash-Cookies“) und Silverlight-Anwendungsspeicher.

Lokal freigegebene Objekte (oder „Flash-Cookies“) Webseiten, die mit Adobe-Flash-Technologien arbeiten, können lokal freigegebene Objekte (oder „Flash-Cookies“) nutzen, um Daten auf Ihrem Computer zu speichern. Rufen Sie zum Verwalten und Blockieren von Flash-Cookies

www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html auf.

Silverlight-Anwendungsspeicher Webseiten oder Apps, die mit der Microsoft-Silverlight-Technologie arbeiten, sind auch in der Lage, Daten im Silverlight-Anwendungsspeicher abzulegen. Informationen zum Verwalten oder Blockieren dieses Speichers finden Sie im Abschnitt [Silverlight](#) in diesen Bestimmungen.

Hinweis für Endbenutzer

Viele Microsoft-Produkte sind für die Verwendung von Organisationen bestimmt und werden von Ihrer Organisation verwaltet. Ihre Nutzung der Microsoft-Produkte unterliegt gegebenenfalls den Richtlinien Ihres Unternehmens. Falls Ihr Unternehmen die Verwaltung für die Nutzung der Microsoft-Produkte vornimmt, richten Sie bitte Ihre Privatsphäre-Anfragen an Ihren Administrator. Wenn Sie die sozialen Eigenschaften dieser Produkte verwenden, können andere Benutzer in Ihrem Netzwerk einige Ihrer Aktivitäten sehen. Um mehr über die sozialen Eigenschaften und andere Funktionen zu erfahren, überprüfen Sie bitte die Dokumentation oder den spezifische Hilfeinhalt für dieses Microsoft-Produkt. Microsoft ist nicht für die Datenschutz- oder Sicherheitspraktiken seiner Kunden, die von denen dieser Richtlinien abweichen können, verantwortlich.

Wenn Sie ein eine E-Mail-Adresse verwenden, die von einer mit Ihnen verbundenen Organisation wie z. B. Ihrem Arbeitgeber oder Ihrer Schule bereitgestellt wird für den Zugriff auf Microsoft Onlinedienste verwenden (wie Ihr Arbeitgeber), kann der Inhaber der mit Ihrer E-Mail-Adresse verknüpften Domäne (i) Ihr Konto und die Microsoft Onlinedienste steuern und verwalten und (ii) auf Ihre Daten zugreifen und diese verarbeiten, einschließlich Ihrer Kommunikationsinhalte und Dateien.

Microsoft-Konto

Mit einem Microsoft-Konto können Sie sich sowohl bei den Microsoft-Produkten als auch bei den von Microsoft ausgewählten Partnern anmelden. Wenn Sie Ihr eigenes Microsoft-Konto erstellen, beziehen wir uns auf dieses Konto als ein persönliches Microsoft-Konto. Wenn Sie sich mit einer E-Mail-Adresse von Ihrem Arbeitgeber oder Ihrer Schule bei Produkten anmelden, die Microsoft Azure Active Directory (AAD) verwenden, beziehen wir uns auf dieses Konto als Arbeits- oder Schulkonto.

Erstellung und Verwendung Ihres persönlichen Microsoft-Kontos. Sobald Sie ein persönliches Microsoft-Konto erstellen, werden Sie nach bestimmten, persönlichen Daten gefragt und wir werden Ihnen eine eindeutige ID-Nummer zuweisen, um Ihr Konto und die zugehörigen Informationen zu identifizieren. Während einige Produkte wie z. B. solche, die Zahlungen enthalten einen richtigen Namen erfordern, können Sie sich bei Microsoft-Produkten anmelden und diese verwenden, ohne dass Sie Ihren richtigen Namen angeben müssen. Einige Daten, die Sie bereitstellen, wie beispielsweise Ihr Name der Anzeige, Ihre E-Mail-Adresse und Telefonnummer, können dazu verwendet werden, anderen dabei zu helfen, Sie innerhalb der Microsoft-Produkte zu finden und sich mit Ihnen zu verbinden. Wenn Personen Ihren angezeigten Name, Ihre E-Mail-Adresse oder Telefonnummer kennen, können sie anhand dieser Daten auf Skype nach Ihnen suchen und Ihnen eine Einladung zur Kontaktaufnahme senden. Wenn Sie sich mit der E-Mail-Adresse Ihrer Arbeit oder Schule anmelden, um ein persönliches Microsoft-Konto zu erstellen und Ihr Arbeitgeber oder Ihre Schule verwaltet das Konto mit Azure Active Directory (AAD), müssen Sie die mit Ihrem persönlichen Microsoft-Konto verbundene E-Mail-Adresse aktualisieren, um auch weiterhin auf Microsoft-Produkte zugreifen zu können, die AAD nicht verwenden (beispielsweise Xbox Live).

Anmelden. Sobald Sie sich bei Ihrem Microsoft-Konto anmelden, erstellen wir eine Aufzeichnung dieses Anmeldevorgangs, der das Datum und die Uhrzeit, Informationen über das Produkt, bei dem Sie sich angemeldet haben, Ihren Anmeldenamen, die eindeutige Nummer, die Ihrem Konto zugewiesen wurde, die eindeutige Kennung, die Ihrem Gerät zugewiesen wurde, Ihre IP-Adresse und Ihr Betriebssystem sowie die Browser-Version enthält.

Anmelden bei Microsoft. Das Anmelden bei Ihrem Konto ermöglicht eine verbesserte Personalisierung, bietet nahtlose und konsistente Erfahrungen für Produkte und Geräte und ermöglicht es Ihnen, Zugang zum Cloud-Datenspeicher zu erhalten und diesen zu verwenden, mithilfe der in Ihrem Microsoft-Konto gespeicherten Zahlungsmittel zu bezahlen und andere erweiterte Features und Einstellungen zu nutzen. Sobald Sie sich bei Ihrem Konto anmelden, bleiben Sie solange angemeldet, bis Sie sich abmelden. Wenn Sie Ihr Microsoft-Konto zu einem Windows-Gerät (Version 8 oder höher) hinzufügen, wird Windows Sie bei den Produkten, die das Microsoft-Konto verwenden und auf die Sie auf diesem Gerät Zugriff haben, anmelden. Sobald Sie angemeldet sind, werden einige Produkte Ihren Namen oder Benutzernamen und Ihr Profilfoto als Teil Ihrer Nutzung der Microsoft-Produkte, einschließlich in Ihren Kommunikationen, sozialen Interaktionen und öffentlichen Beiträgen anzeigen (falls Sie diese Ihrem Profil hinzugefügt haben).

Anmelden bei Drittanbieter-Produkten. Wenn Sie sich bei einem Drittanbieter-Produkt mit Ihrem Microsoft-Konto anmelden, werden Sie aufgefordert, Ihre Einwilligung zu geben, um die von diesem Produkt benötigten Kontodaten zu teilen. Der Drittanbieter erhält außerdem die Versionsnummer, die Ihrem Konto zugeordnet wurde (eine neue Versionsnummer wird immer dann zugewiesen, wenn Sie Ihre Anmeldeinformationen ändern); und eine Mitteilung darüber, ob Ihr Konto deaktiviert wurde. Wenn Sie der Freigabe Ihrer Profildaten zugestimmt haben, kann der Drittanbieter möglicherweise Ihren Namen oder Benutzernamen und Ihr Profilfoto (falls Sie es Ihrem Profil hinzugefügt haben) anzeigen, wenn Sie bei dem Drittanbieter-Produkt angemeldet sind. Wenn Sie mithilfe Ihres

Microsoft-Kontos Zahlungen an Drittanbieter durchführen möchten, gibt Microsoft die in Ihrem Microsoft-Konto gespeicherten Informationen an Drittanbieter weiter, damit Ihre Zahlung verarbeitet und Ihre Bestellung ausgeführt werden kann (z. B. den Namen, eine Kreditkartennummer, Rechnungs- und Lieferadressen und relevante Kontaktinformationen). Der Drittanbieter kann die von Ihnen bei der Anmeldung oder beim Kauf eingegebenen Daten gemäß seiner eigenen Praxis und Richtlinien nutzen. **Sie sollten die Datenschutzerklärung eines jeden Produktes, bei dem Sie sich anmelden und von jedem Händler, von dem Sie etwas erwerben, sorgfältig lesen, um zu erfahren, wie die erfassten Daten verwendet werden.**

Von Drittanbietern erhaltene persönliche Microsoft-Konten. Wenn Sie Ihr persönliches Microsoft-Konto von einem Drittanbieter, z. B. einem Internetprovider, erhalten haben, dann kann dieser Drittanbieter möglicherweise die Rechte an Ihrem Konto besitzen, einschließlich der Möglichkeit, auf das Microsoft-Konto zuzugreifen oder es zu löschen. **Sie sollten alle weiteren, Ihnen durch Drittanbieter angebotenen Bedingungen sorgfältig prüfen, um zu verstehen, welche Konsequenzen diese für Ihr Konto haben.**

Nutzung von Arbeits- und Schulkonten. Wenn Ihr Arbeitgeber oder Ihre Schule Azure Active Directory (AAD) für das für Sie bereitgestellte Konto verwendet, können Sie dieses Konto zur Anmeldung bei Microsoft-Produkten nutzen, die AAD verwenden (z. B. Office 365 oder Skype for Business). Falls von Ihrer Organisation gefordert, werden Sie gebeten, eine Telefonnummer oder eine alternative E-Mail-Adresse als zusätzliche Sicherheitsüberprüfung anzugeben. Wenn Sie sich bei Microsoft-Produkten mit einem Arbeits- oder Schulkonto anmelden, kann der Besitzer, der mit Ihrer E-Mail-Adresse verbundenen Domäne, Ihr Konto sowie den Zugang zu Ihren Daten und die Verarbeitung Ihrer Daten, einschließlich der Inhalte Ihrer Mitteilungen und Dateien, kontrollieren und administrieren. Ihre Nutzung der Produkte unterliegt gegebenenfalls den Richtlinien Ihres Unternehmens. Microsoft ist für die Datenschutz- oder Sicherheitspraktiken dieser Organisationen, die sich von denen von Microsoft unterscheiden können, nicht verantwortlich. Falls Ihr Unternehmen die Verwaltung für die Nutzung von Microsoft-Produkten vornimmt, richten Sie bitte Ihre Privatsphäre-Anfragen an Ihren Administrator. Weitere Informationen finden Sie unter [Hinweis für Endbenutzer](#).

Weitere Wichtige Informationen zum Datenschutz

Nachfolgend finden Sie zusätzliche Datenschutzinformationen, die Sie möglicherweise für wichtig halten. Weitere Informationen zum Engagement von Microsoft für den Schutz Ihrer Privatsphäre finden Sie auch unter privacy.microsoft.com.

Europäische Datenschutzrechte

Microsoft hält sich an geltende Datenschutzgesetze des europäischen Wirtschaftsraums, die, sofern zutreffend, über die folgenden Rechte verfügen:

- Wenn die Verarbeitung von persönlichen Daten auf Ihrer Zustimmung beruht, haben Sie das Recht, Ihre Zustimmung jederzeit für zukünftige Käufe zu widerrufen.

- Sie haben das Recht, von uns einen gemäß den Richtlinien definierten „Daten-Controller“ für den Zugriff auf und die Beseitigung Ihrer persönlichen Daten anzufordern.
- Sie können gegen die Verarbeitung Ihrer persönlichen Daten Einspruch erheben und
- Sie haben das Recht, bei einer Datenschutzbehörde eine Beschwerde einzureichen.

Nach Französischem Recht können Sie uns hier ebenfalls spezifische Anweisungen über die Verwendung Ihrer persönlichen Daten nach Ihrem Tod senden:

[Webformular](#) .

Wenn wir persönliche Daten über Sie einholen, geschieht dies mit Ihrer Zustimmung oder nach Bedarf, um die von Ihnen verwendeten Produkte anzubieten, für unsere Geschäftstätigkeit, zur Erfüllung unserer vertraglichen und gesetzlichen Verpflichtung, um die Sicherheit unserer Systeme und unserer Kunden zu gewährleisten oder andere berechnigte Interessen von Microsoft zu erfüllen, wie in den Abschnitten „Wie wir personenbezogene Daten nutzen“ und „Gründe, Warum Wir persönliche Daten Teilen“ oben beschrieben. Wenn wir persönliche Daten aus dem europäischen Wirtschaftsraum beziehen, geschieht dies aufgrund einer Vielzahl von gesetzlichen Mechanismen, wie im Abschnitt „Wo wir personenorientierte Daten speichern“ weiter unten beschrieben.

Die Sicherheit personenbezogener Daten

Microsoft sorgt für die Sicherheit Ihrer personenbezogenen Daten. Wir verwenden eine Reihe unterschiedlicher Sicherheitstechnologien und -verfahren, um Ihre personenbezogenen Daten vor unbefugtem Zugriff, Missbrauch oder unzulässiger Offenlegung zu schützen. Ihre personenbezogenen Daten werden von uns z. B. auf Computersystemen an kontrollierten Standorten und mit begrenztem Zugriff gespeichert. Wenn wir personenbezogene Daten (wie Kreditkartennummern oder Kennwörter) über das Internet übertragen, werden diese von uns durch Verschlüsselungstechniken geschützt.

Wo wir personenorientierte Daten speichern und verarbeiten

Die von Microsoft gesammelten, personenbezogenen Daten können in Ihrer Region, in den USA oder in jedem anderen Land gespeichert und verarbeitet werden, in dem Microsoft oder seine Tochterunternehmen Niederlassungen oder ihre Dienstleister-Einrichtungen unterhalten. Microsoft verwaltet großen Rechenzentren in Australien, Österreich, Brasilien, Kanada, Finnland, Frankreich, Deutschland, Hong Kong, Indien, Irland, Japan, Korea, Malaysia, den Niederlanden, Singapur, dem Vereinigten Königreich und den USA. In der Regel befindet sich der primäre Speicherort in der Region des Kunden oder in den Vereinigten Staaten, mit einer Datensicherung in einem Rechenzentrum in einer anderen Region. Die Speicherorte werden effizient, zur Verbesserung der Leistung und zum Erstellen

von Redundanzen ausgewählt, um die Daten im Falle eines Stromausfalls oder bei einem anderen Problem zu schützen. Wir unternehmen Schritte, um sicherzustellen, dass die Daten, die wir im Rahmen dieser Datenschutzerklärung sammeln, den Bestimmungen dieser Erklärung und den Anforderungen an das geltende Recht entsprechen, wo immer sich diese Daten auch befinden.

Wir übertragen persönliche Daten aus dem Europäischen Wirtschaftsraum und der Schweiz in andere Länder, von denen einige von der Europäischen Kommission nicht als Länder mit angemessenem Datenschutz festgelegt wurden. In diesem Fall verwenden wir eine Vielzahl von gesetzlichen Mechanismen, einschließlich Verträge, um sicherzustellen, dass Ihre Rechte und der Schutz Ihrer übertragenen Daten gewährleistet ist. Weitere Informationen zu den Entscheidungen der Europäischen Kommission über den Schutz der persönlichen Daten in den Ländern, in denen Microsoft personenbezogene Daten verarbeitet:

ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Die Microsoft Corporation hält das vom US Department of Commerce dargelegte EU-US Privacy Shield-Rahmenabkommen bezüglich der Erfassung, Nutzung und Speicherung von personenbezogenen, aus der Europäischen Union und der Schweiz in die USA übertragenen Daten ein. Die Microsoft Corporation hat gegenüber dem Department of Commerce zertifiziert, dass es die Privacy Shield-Prinzipien einhält. Wenn Drittanbieter personenbezogene Daten in unserem Namen in einer Weise verarbeiten, die mit den Prinzipien jedes Privacy Shield-Abkommens unvereinbar sind, bleiben wir haftbar, sofern wir nicht beweisen können, dass wir für das Ereignis, das den Schaden verursacht hat, nicht verantwortlich sind. Die kontrollierten U.S.-Tochtergesellschaften der Microsoft Corporation, die in unserer Selbstzertifizierungsvorlage genannt und in [hier](#) aufgeführt werden, halten sich ebenfalls an die Privacy Shield-Prinzipien.

Wenn Konflikte zwischen den Bestimmungen in dieser Datenschutzrichtlinie und den Privacy Shield-Prinzipien auftreten, haben die Privacy Shield-Prinzipien Vorrang. Weitere Informationen zum Privacy Shield-Programm und zu unserer Zertifizierung finden Sie unter www.privacyshield.gov.

Wenn Sie eine Frage oder eine Beschwerde im Zusammenhang mit der Teilnahme von Microsoft am EU-US oder Schweiz-US Privacy Shield-Abkommen haben, wenden Sie sich bitte an uns unter [Webformular](#). Für alle Beschwerden im Zusammenhang mit den Privacy Shield-Abkommen, die nicht direkt mit Microsoft gelöst werden können, haben wir uns entschlossen, mit der jeweiligen Datenschutzbehörde zusammenzuarbeiten, die von den europäischen Datenschutzbehörden für die Beilegung von Streitigkeiten eingerichtet wurde. Wir leiten Sie gerne an die relevanten Kontakte in den Datenschutzbehörden weiter. Bitte sprechen Sie uns an. Wie bereits in den Privacy Shield-Grundsätzen beschrieben, gibt es ein bindendes Schiedsverfahren für Beschwerden, die auf andere Art und Weise nicht zu lösen sind. Microsoft unterliegt den Untersuchungs- und Vollstreckungsbefugnissen der U.S. Federal Trade Commission (FTC).

Unsere Vorgehensweise bei der Speicherung persönlicher Daten

Microsoft speichert persönliche Daten so lange wie es nötig ist Produkte zu erbringen und Transaktionen zu vollenden, die Sie angefordert haben oder für andere wichtige Zwecke, wie die Einhaltung unserer gesetzlichen Verpflichtung, Streitbeilegung und für die Durchsetzung unserer Verträge. Da diese Maßnahmen für andere Datentypen im Kontext anderer Produkten variieren, kann die tatsächliche Aufbewahrungsdauer erheblich variieren. Die Kriterien, die die Aufbewahrungsdauer ermitteln sind wie folgt:

- *Wie lange sind die persönlichen Daten für das Angebot der Produkte und unserer Geschäftstätigkeit nützlich?* Dazu gehören z. B. die Erhaltung und Verbesserung der Leistung dieser Produkte, die Sicherheit unserer Systeme und das sachgerechte Verwalten der Geschäftstätigkeiten und Finanzdaten. Dies ist die allgemeine Regel für die Basis der Datenaufbewahrungsdauer.
- *Hat der Kunde die Daten mit der Erwartung angegeben, erstellt und verwaltet, dass wir diese so lange behalten, bis wir von ihm zum Entfernen aufgefordert werden?* Dazu gehören: Dokumente, die Sie auf OneDrive speichern oder eine E-Mail-Nachricht, die Sie im Posteingang von Outlook.com aufbewahren. In diesem Fall werden die Daten beibehalten, bis Sie diese selbst löschen, z.B. wenn Sie eine E-Mail aus Ihrem Posteingang in Outlook.com in den Ordner „Gelöschte Objekte“ verschieben und diesen Ordner anschließend leeren (wenn der Ordner „Gelöschte Objekte“ geleert wird, bleiben die gelöschten Elemente in unserem System für bis zu 30 Tage erhalten, bevor sie endgültig gelöscht werden).
- *Gibt es eine automatische Kontrolle, z. B. im Microsoft-Datenschutz-Dashboard, mit dem Kunden Zugriff auf persönlichen Daten haben und diese jederzeit löschen können?* Wenn dies nicht der Fall ist, wird in der Regel eine kürzere Datenaufbewahrungszeit verwendet.
- *Sind persönliche Daten sensible Datentypen?* Wenn dies nicht der Fall ist, wird in der Regel eine kürzere Datenaufbewahrungszeit verwendet.
- *Wendet Microsoft eine bestimmte Aufbewahrungsdauer für einen bestimmten Datentyp an?* Für Bing-Suchanfragen führen wir beispielsweise eine De-Identifizierung von gespeicherten Abfragen durch, indem die vollständige IP-Adresse nach 6 Monaten und Cookie-IDs und andere sitzungsübergreifende Kennungen nach 18 Monaten gelöscht werden.
- *Stimmt der Benutzer einer längeren Aufbewahrungsdauer zu?* Wenn dies der Fall ist, bewahren wir die Daten mit Ihrer Zustimmung auf.
- *Hat Microsoft eine rechtliche, vertragliche oder ähnliche Verpflichtung, die Daten aufzubewahren?* Beispiele sind etwa: gesetzliche Datenaufbewahrungsgesetze in zutreffenden Gerichtsbarkeiten, staatliche Gesetze zur Aufbewahrung relevanter Daten im Falle einer Untersuchung, die zum Zweck der Rechtsstreitigkeiten aufbewahrt werden müssen.

Vorschau oder kostenlose Veröffentlichungen

Microsoft bietet Vorschau-Optionen, Insider, Beta – oder kostenlose Versionen oder andere Funktionen und Produkte vor der allgemeinen Veröffentlichung („Vorschau“) an, damit Sie diese Vorabveröffentlichungen auswerten und Microsoft eine Rückmeldung dazu geben können, auch bezüglich Leistungs- und Nutzungsdaten. Als Ergebnis können Vorschau-Optionen automatisch zusätzliche Daten sammeln, weniger Kontrollelemente bereitstellen und auch sonst andere Datenschutz- und Sicherheitsmaßnahmen verwenden als diejenigen, welche typischerweise bei unseren Produkten verwendet werden. Wenn Sie sich an Vorschau-Optionen beteiligen, nehmen wir möglicherweise mit Ihnen Kontakt bezüglich Ihrer Rückmeldung oder Ihres Interesses an der Nutzung des besagten Produkts nach deren allgemeiner Veröffentlichung auf.

Änderungen an dieser Datenschutzerklärung

Wir werden diese Datenschutzerklärung von Zeit zu Zeit aktualisieren, um das Feedback von Kunden sowie Änderungen bei den Produkten zu berücksichtigen. Wenn Änderungen an den Bestimmungen vorgenommen wurden, können Sie das anhand des geänderten Datums unter „Letzte Aktualisierung“ am Anfang der Datenschutzbestimmungen erkennen. Die Änderungen werden ebenfalls unter [Änderungsverlauf](#) beschrieben. Bei grundlegenden Änderungen oder bei Änderungen in Bezug auf die Verwendung Ihrer persönlichen Daten durch Microsoft, wird entweder vor der Implementierung dieser Änderungen an hervorgehobener Stelle ein Hinweis angezeigt oder Sie erhalten direkt von Microsoft eine Benachrichtigung. Sie sollten diese Datenschutzbestimmungen deshalb regelmäßig überprüfen, um zu erfahren, wie Microsoft Ihre personenbezogenen Daten schützt.

So erreichen Sie uns

Rufen Sie bei Technik- oder Supportfragen support.microsoft.com auf, um mehr über die Microsoft-Supportangebote zu erfahren. Rufen Sie [Support für Microsoft-Konten](#) auf, wenn Sie eine Frage zum Kennwort eines persönlichen Microsoft-Kontos haben.

Wenn Sie Fragen oder Beschwerden zum Thema Datenschutz oder eine Frage an den Chief Privacy Officer/Datenschutzbeauftragten von Microsoft haben, wenden Sie sich bitte unter [Webformular](#) an uns. Wir beantwortet Fragen oder sonstige Anliegen innerhalb von 30 Tagen.

Soweit nicht anderweitig angegeben, ist die Microsoft Corporation die für die Verarbeitung Verantwortliche für die persönlichen Daten, die wir über die Produkte sammeln, die Gegenstand dieser Bestimmungen sind. Unsere Adresse lautet Microsoft Privacy, Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, USA. Telefon: (+1) 425-882-8080.

Die Microsoft Ireland Operations Limited ist unsere Datenschutzbeauftragte für den Europäischen Wirtschaftsraum und die Schweiz. Den Datenschutzbeauftragten von

Microsoft Ireland Operations Limited erreichen Sie unter folgender Anschrift:
Microsoft Ireland Operations, Ltd., Attn: Data Protection, Carmenhall Road,
Sandyford, Dublin 18, Irland.

Skype Communications S.à.r.l. 23-29 Rives de Clausen L-2165 Luxemburg,
Luxemburg ist die für die Verarbeitung Verantwortliche Stelle für Skype. Wenn Sie
sich bezüglich Skype-Software oder -Produkten an uns wenden möchten, richten
Sie eine Supportanfrage an das [Kundensupportteam](#) von Skype.

Informationen zu den Microsoft-Niederlassungen in Ihrem Land oder in Ihrer
Region finden Sie unter www.microsoft.com/worldwide/.

Produkte für Unternehmen und Entwickler

Produkte für Unternehmen und Entwickler sind Microsoft-Produkte und ähnliche Software,
die in erster Linie für Organisationen oder Entwickler angeboten und konzipiert sind. Diese
Supportoptionen umfassen:

- Dazu gehören Clouddienste, die auch Onlinedienste genannt werden im [Geschäftsbedingungen für Microsoft Onlinedienste](#) (OST), wie Office 365, Microsoft Azure, Microsoft Dynamics365, Microsoft Intune und Yammer, für deren Dienste („Enterprise-Onlinedienste“) eine Organisation (unser Kunde) Verträge mit Microsoft eingegangen ist.
- Server und Entwickler-Produkte wie z. B. Windows Server, SQL Server, Visual Studio und System Center („Software für Unternehmen und Entwickler“).
- Appliances und Hardware für die Speicherinfrastruktur, z. B. StorSimple („Enterprise Appliances“); und
- Cognitive Services wie z. B. Emotion-API, Bing-Spracheingabe-API, Empfehlungen-API, für die ein Unternehmen oder Entwickler (unser Kunde) Verträge mit Microsoft Services („Cognitive Services“) abschließt.
- Entwicklerdienste wie Bot Framework, Cortana Skills Kit und Botlet Store.

Im Falle eines Konflikts zwischen diesen Microsoft-Datenschutzbestimmungen und den Bedingungen einer bzw. mehrerer Vereinbarung(en) zwischen einem Kunden und Microsoft für Produkte für Unternehmen und Entwickler, sind die Bedingungen dieser Vereinbarung(en) ausschlaggebend.

In der Produktdokumentation erhalten Sie ebenfalls Informationen über die Funktionen und Einstellungen unserer Produkte für Unternehmen und Entwickler, einschließlich der Optionen, die Auswirkungen auf Ihre Privatsphäre oder den Datenschutz unserer Endbenutzer haben.

Falls die unten aufgeführten Bestimmungen nicht in dieser Datenschutzerklärung aufgeführt sind oder im [OST](#), finden Sie die Definitionen weiter unten.

Allgemein. Wenn ein Kunde die Produkte für Unternehmen und Entwickler ausprobiert, kauft, verwendet oder abonniert oder Unterstützung für diese Produkte erhält, erfasst

Microsoft Daten für diesen Service, um die besten Erfahrungen mit unseren Produkten zu bieten, unser Geschäft zu führen und mit dem Kunden zu kommunizieren. Zum Beispiel:

- Wenn ein Kunde mit einem Microsoft Vertriebsmitarbeiter zusammen arbeitet, erfassen wir den Namen des Kunden und die Kontaktdaten zusammen mit Informationen über das Unternehmen des Kunden, das diesen Auftrag unterstützt.
- Wenn ein Kunde mit einem Support-Mitarbeiter von Microsoft interagiert, erfassen wir diese Geräte- und Nutzungsdaten oder Fehlerberichte, um Probleme zu diagnostizieren und beheben.
- Wenn ein Kunde für die Produkte zahlt, erfassen wir die Kontaktinformationen und Zahlungsdaten.
- Wenn ein Kunde Mitteilungen von Microsoft erhält, verwenden wir die Daten zur Personalisierung des Inhalts der Mitteilung.

Mit den Produkten für Unternehmen und Entwickler können Sie andere Produkte und Onlinedienste mit unterschiedlichen Datenschutzpraktiken von Microsoft oder von Drittanbietern erwerben, abonnieren oder verwenden. Diese anderen Produkte und Onlinedienste unterliegen ihren jeweiligen Datenschutzbestimmungen und Richtlinien.

Enterprise Onlinedienste

Um die Enterprise-Onlinedienste anzubieten, erfasst Microsoft Kundendaten, Administratordaten, Zahlungsdaten und Support-Daten.

Wir verwenden die Kundendaten und die Support-Daten wir in [OST](#) und in [Microsoft Trust Center](#) beschrieben.

„Administratordaten“ sind Informationen, die Microsoft während der Anmeldung, dem Erwerb oder der Verwaltung der Enterprise-Onlinedienste zur Verfügung gestellt werden. Wir verwenden Administratordaten, um Enterprise-Onlinedienste, komplette Transaktionen sowie die Wartung des Kontos anzubieten, und um einen Betrug zu erkennen und zu verhindern. Administratordaten enthalten den Namen, die Adresse, Telefonnummer und E-Mail-Adresse, die von Ihnen zur Verfügung gestellt werden sowie aggregierte Nutzungsdaten Ihres Kontos, wie beispielsweise die von Ihnen ausgewählten Steuerelemente. Administratordaten können auch Kontaktinformationen Ihrer Kollegen und Freunde enthalten, falls Sie damit einverstanden sind, diese Microsoft, für den begrenzten Zweck der Zusendung einer Einladung für die Enterprise- Onlinedienste, zu liefern. Wir werden diese Personen möglicherweise mit Informationen über Sie kontaktieren, wie beispielsweise Ihrem Namen und Ihrem Profilfoto.

Bei Bedarf werden wir Administratordaten verwenden, um Sie zu kontaktieren, und um Informationen über ihre Konto-Mitgliedschaften, Rechnungsstellung und Aktualisierungen der Enterprise-Onlinedienste, einschließlich Informationen über neue Funktionen, die Sicherheit oder andere technische Probleme anzubieten. Wir werden Sie möglicherweise bezüglich Anfragen von Dritten kontaktieren, die wir aus Ihrer Verwendung der Enterprise-Onlinedienste erhalten, wie im Vertrag

festgelegt. Sie können sich von diesen werbungsfreien Kommunikationen nicht abmelden. Je nach Ihren Kontaktpräferenzen können wir Sie auch bezüglich Informationen und Angeboten über andere Produkte und - Dienstleistungen kontaktieren oder Ihre Kontaktinformationen mit Microsoft-Partnern teilen. Sie können Ihre Kontaktpräferenzen verwalten oder Informationen in ihrem Kontoprofil aktualisieren.

Wir verwenden Zahlungsdaten, um Onlinedienste und komplette Transaktionen anzubieten, und um einen Betrug zu erkennen und zu verhindern.

Einige Enterprise-Onlinedienste erfordern oder werden durch die Installation von lokaler Software (z. B. Agenten, Anwendungen für Geräteverwaltung) auf einem Gerät verbessert. Nach Wunsch kann die lokale Software (i) Daten übertragen, inklusive Kundendaten von einem Gerät oder einer Anwendung zu oder von Enterprise-Onlinediensten; oder (ii) Protokolle oder Fehlerberichte für Microsoft zur Problembehandlung. Der Enterprise-Onlinedienste, einschließlich der lokalen Software, erfassen möglicherweise auch Geräte- und Nutzungsdaten, die an Microsoft übermittelt und analysiert werden, um die Qualität, Sicherheit und Integrität unserer Produkte zu verbessern.

Software für Unternehmen und Entwickler und Enterprise Appliances

Software für Unternehmen und Entwickler und Enterprise Appliances sammeln Daten, um einen effektiven Betrieb zu garantieren und Ihnen die besten Erfahrungen zu bieten. Die Daten, die wir erheben, hängen zwar von den Ihnen verwendeten Funktionen sowie der Konfiguration und den Einstellungen ab, sie sind allerdings in der Regel auf Geräte- und Nutzungsdaten beschränkt. Kunden haben die Wahl zu bestimmen, welche Daten sie bereitstellen möchten. Zum Beispiel:

- Während der Installation oder beim Ausführen eines Upgrades für eine Entwickler- oder Unternehmenssoftware erfassen wir möglicherweise Geräte- und Nutzungsdaten, um zu erfahren, ob diese Ihnen Probleme bereiten.
- Wenn Sie Software oder Appliances für Unternehmen verwenden, erfassen wir möglicherweise Geräte- und Nutzungsdaten zur Verbesserung der Sicherheitsfunktionen Ihrer Betriebsumgebung.
- Bei einem Absturz mit der Software oder Appliances für Unternehmen können Sie Microsoft einen Fehlerbericht senden, damit wir das Problem diagnostizieren und Kundensupport anbieten können.

Microsoft verwendet die von der Software für Unternehmen und Entwickler sowie Enterprise Appliances erfassten Daten, um unsere Produkte zu verbessern, Kundensupport zum Aktivieren des Produkts anzubieten, mit Ihnen zu kommunizieren und für unsere Geschäftstätigkeit.

Microsoft SQL Server ist ein relationales Datenbankmanagementsystem und umfasst Produkte, die separat installiert werden können (z. B. SQL Server

Management Studio). Detaillierte Informationen darüber, welche Daten wir sammeln, wie wir sie nutzen und wie Sie Ihre Datenschutzoptionen verwalten können, finden Sie unter [SQL Server-Datenschutzeroptionen hier](#). Wenn Sie in einem Unternehmen arbeiten, kann Ihr Administrator bestimmte Einstellungen für Telemetrie über Gruppenrichtlinien festlegen.

Cognitive Services

Mit Microsoft Cognitive Services können Entwickler Anwendungen erstellen, die Daten besser auswerten können, beispielsweise durch Erkennen von Gesichtern und Objekten in Bildern, Verstehen von gesprochenen Wörtern oder Interpretieren von Befehlen. Wir sammeln und verwenden Ihre Daten für die Bereitstellung der Dienste sowie zur Verbesserung und Personalisierung Ihrer Erfahrung.

Cognitive Services sammelt und verwendet viele Arten von Daten, beispielsweise Bilder, Audiodateien, Videodateien und Texte. Alle diese Daten werden von Microsoft gespeichert. Microsoft hat geschäftliche und technische Maßnahmen implementiert, die dazu dienen, einige Cognitive Services-Daten unkenntlich zu machen. Durch Unkenntlichmachung werden Daten nicht vollständig anonymisiert. Beispielsweise kann eine Person in einem Foto noch von einem Betrachter erkannt werden, der die Person kennt.

Microsoft und Apps, die Cognitive Services verwenden, sammeln und verwenden möglicherweise Ihre Daten. Beispielsweise verwendet Bing Suchabfragen, die über die Bing-Such-APIs der Cognitive Services gesammelt wurden, wie im Abschnitt „Bing“ beschrieben. Microsoft Translator verwendet Daten, die über die Translator-API der Cognitive Services gesendet werden, wie im Abschnitt „Translator“ beschrieben.

Produktivitäts- und Kommunikationsprodukte

Produktivitäts- und Kommunikationsprodukte sind Anwendungen, Software und Dienste, die Sie zum Erstellen, Speichern und Freigeben von Dokumenten verwenden und um mit anderen zu kommunizieren.

Office

Office ist eine Sammlung an produktiven Apps einschließlich Word, Excel, PowerPoint und Outlook. Weitere Details zu Outlook finden Sie unter [Outlook](#) in den Datenschutzbestimmungen. Verschiedene Office-Apps ermöglichen es Ihnen, Inhalte und Funktionen zu nutzen, die mit anderen Microsoft- und Drittanbieterdiensten, wie Bing, verbunden sind. Ausführliche Informationen zur Verwaltung Ihrer Datenschutzoptionen finden Sie unter go.microsoft.com/fwlink/?LinkId=624445. Wenn Sie in einem Unternehmen arbeiten, kann Ihr Administrator verbundene Dienste über die Gruppenrichtlinie deaktivieren.

Office-Roamingdienst. Der Office-Roamingdienst hilft Ihnen dabei, Ihre Office-Einstellungen auf allen mit Office betriebenen Geräten auf dem neuesten Stand zu halten. Wenn Sie sich mit Ihrem [Microsoft-Konto](#) bei Office anmelden, wird der Office-Roamingdienst aktiviert. Dabei werden einige Ihrer benutzerdefinierten Office-Einstellungen mit Microsoft-Servern synchronisiert (z. B. eine Liste der zuletzt verwendeten Dokumente und die zuletzt angezeigte Position innerhalb eines Dokuments). Wenn Sie sich bei Office an einem anderen Gerät mit demselben Konto anmelden, lädt der Office Roamingdienst Ihre Einstellungen von den Microsoft-Servern herunter und wendet diese bei dem zusätzlichen Gerät an. Der Office Roaming-Dienst verwendet auch einige Ihrer benutzerdefinierten Office-Einstellungen, sobald Sie sich bei Office.com anmelden. Wenn Sie sich bei Office abmelden, entfernt der Office Roaming-Dienst Ihre Office-Einstellungen von Ihrem Gerät. Alle durch Sie in Ihren benutzerdefinierten Office-Einstellungen vorgenommenen Änderungen werden an die Microsoft-Server gesendet.

Microsoft Updates. Office verwendet den [Microsoft Update](#) Service, um Ihnen Updates für die Sicherheit und weitere wichtige Updates zur Verfügung zu stellen. Im Abschnitt „Aktualisierungsdienst“ dieser Datenschutzerklärung finden Sie weitere Informationen.

Online-Hilfe, Vorlagen, Schriftarten und weitere Inhalte. Office verwendet weitere Microsoft- oder Drittanbieter-Dienste, um Ihnen die neuesten Online-Inhalte zukommen zu lassen, wenn Sie mit dem Internet verbunden sind wie beispielsweise Hilfeartikel, Vorlagen und Schriftarten. Sobald Sie beispielsweise das Hilfe-Feature in den Office-Apps verwenden, sendet Office Ihre Suchabfrage an Office.com, um Sie mit Online-Hilfe-Elementen zu versorgen. Diese Features sind standardmäßig aktiviert, aber Sie können sie auch unter Verwendung der Datenschutzeinstellungen deaktivieren. Sie können auf die Datenschutzeinstellungen in Office 2013 zugreifen, indem Sie auf **Datei > Optionen > Trust Center > Trust Center-Einstellungen > Datenschutzoptionen klicken**

Click-to-Run-Aktualisierungsdienst. Der Click-to-Run-Aktualisierungsdienst erlaubt es Ihnen, bestimmte Microsoft Office-Produkte über das Internet zu installieren, so dass Sie mit ihrer Verwendung beginnen können, bevor diese vollständig heruntergeladen sind. Von Hause aus ist der Click-to-Run-Aktualisierungsdienst auch automatisch in der Lage, Online-Aktualisierungen für Click-to-Run-fähige Produkte auf Ihrem Gerät zu erkennen und diese automatisch herunterzuladen und zu installieren. Dieser Dienst ist standardmäßig aktiviert. Sie können ihn jedoch unter Verwendung der Datenschutzeinstellungen deaktivieren.

Suchdienste. Von Office unterstützte Suchdienste, wie beispielsweise Insights, erlauben es Ihnen, Informationen von Microsoft- oder Drittanbieterdiensten innerhalb einer Office-App anzufordern. Sie können zum Beispiel in Word ein Wort oder einen Satz markieren und so relevante Informationen aus Bing abrufen. Wenn Sie nach einem bestimmten Wort oder einer Wendung suchen, sendet Office den von Ihnen angeforderten Text verschlüsselt an den Dienst (und bei der

Verwendung von Insights wird Office, um Ihnen die im Kontext relevanten Suchergebnisse bereitzustellen, das angeforderte Wort oder die Wendung mit einigen umliegenden Inhalten aus Ihrem Dokument senden). In Excel können Sie Kategorien von Daten an Microsoft senden, um Empfehlungen für andere Sätze an ähnlichen Daten zu erhalten, die Sie interessieren könnten, aber der tatsächliche Inhalt Ihres Arbeitsbuchs wird nicht an Microsoft gesendet. Außerdem sendet Office Daten über die Software, die Sie verwenden, und das auf Ihrem System eingestellte Gebietsschema. Falls von einem Drittanbieter von Inhalten angefordert, sendet es auch Autorisierungsdaten, die angeben, dass Sie dazu berechtigt sind, die jeweiligen Inhalte herunterzuladen. Häufig enthält die erhaltene Information einen Link, welcher Sie zu weiteren Informationen auf der Webseite des Inhaltsanbieters leitet. Wenn Sie auf den Link klicken, wird der Anbieter der Inhalte möglicherweise ein [Cookie](#) auf Ihrem Gerät setzen, um Sie bei zukünftigen Transaktionen identifizieren zu können.

Übersetzungsdienst. Einige Office-Apps erlauben es Ihnen, einen Teil oder das gesamte Dokument mit Hilfe eines zweisprachigen Wörterbuchs oder einer maschinellen Übersetzung zu übersetzen. Sollte ein Wort oder ein Satz, den Sie übersetzen möchten, nicht im zweisprachigen Wörterbuch Ihrer App enthalten sein, wird das Wort oder der Satz unverschlüsselt an einen Microsoft- oder einen Drittanbieter-Übersetzungsdienst gesendet. Wenn Sie sich dafür entscheiden, das gesamte Dokument zu übersetzen, wird das gesamte Dokument unverschlüsselt an einen Microsoft- oder einen Drittanbieter-Übersetzungsdienst gesendet. Zusätzlich zu dem Wort oder dem Satz, den Sie übersetzen wollen, sendet Office Informationen über die von Ihnen verwendete Office-Software, einschließlich Version, Betriebssystem, Region und Sprache, auf die Ihr System eingestellt ist. Im Falle von Übersetzungsdiensten durch Drittanbieter, sendet Office möglicherweise auch eine zuvor gespeicherte Authentifizierungsinformationen, welche bescheinigt, dass Sie sich bereits zuvor für den Zugang zu der Webseite registriert hatten.

OneDrive

Microsoft OneDrive ermöglicht es Ihnen auf jedem Gerät zu Speichern und auf Ihre Dateien zuzugreifen. Sie können Dateien auch mit anderen teilen und gemeinsam bearbeiten. Bei einigen Versionen der Microsoft OneDrive-Anwendung können Sie sowohl auf Ihr persönliches OneDrive zugreifen, indem Sie sich bei Ihrem persönlichen Microsoft-Konto anmelden, als auch auf Ihr OneDrive for Business, indem Sie sich mit Ihrem Arbeits- oder Schulkonto von Microsoft im Rahmen der Office 365-Nutzung Ihres Unternehmens anmelden.

Wenn Sie OneDrive verwenden, werden wir die Daten, die Sie bei diesem Dienst verwendet haben sowie die von Ihnen gespeicherten Inhalte erheben, um Ihnen die Dienste bereitzustellen, diese zu verbessern und zu schützen. Beispiele umfassen sowohl die Indizierung Ihrer OneDrive-Dokumente, so dass Sie diese später durchsuchen können als auch die Verwendung von Ortsinformationen, um Ihnen die Suche nach Fotos auf Basis der Orte, wo das Foto aufgenommen wurde, zu

erleichtern. Wir erheben zudem Geräteinformationen, damit wir personalisierte Erfahrungen liefern können, wie beispielsweise die Synchronisation der Inhalte auf den Geräten und das Durchsuchen benutzerdefinierter Einstellungen.

Sobald Sie Inhalte in Microsoft OneDrive speichern, werden die Inhalte die Freigabeberechtigungen der Ordner übernehmen, in den Sie den Inhalt speichern. Wenn Sie beispielsweise Inhalte im öffentlichen Ordner speichern, wird der Inhalt der Öffentlichkeit und für jeden im Internet zugänglich, der diesen Ordner finden kann. Wenn Sie Inhalte in einem privaten Ordner speichern, wird der Inhalt als privat gehandhabt.

Wenn Sie Inhalte auf einem sozialen Netzwerk wie Facebook von einem Telefon teilen, das mit Ihrem Microsoft OneDrive Konto synchronisiert wurde, dann werden Ihre Inhalte entweder auf dieses Netzwerk hochgeladen oder es wird ein Link zu diesem Inhalt auf diesem Netzwerk eingesetzt. Auf sozialen Netzwerken veröffentlichte und auf Microsoft OneDrive gehostete Inhalte sind für jedermann in diesem sozialen Netzwerk zugänglich. Um den Inhalt zu löschen, müssen Sie ihn vom sozialen Netzwerk und vom Microsoft OneDrive löschen.

Wenn Sie Ihre Microsoft OneDrive Inhalte mit Ihren Freunden über einen Link freigeben, wird eine E-Mail mit diesem Link an diese Freunde gesendet. Der Link enthält einen Autorisierungscode, der jedem der diesen Link erhält, einen Zugriff auf Ihre Inhalte ermöglicht. Wenn einer Ihrer Freunde diesen Link an weitere Personen sendet, dann werden auch diese in der Lage sein, auf Ihre Inhalte zuzugreifen, auch wenn Sie diesen Inhalt mit ihnen nicht teilen wollten. Um Berechtigungen für Ihre Inhalte auf Microsoft OneDrive zu widerrufen, melden Sie sich an Ihrem Konto an, und wählen Sie dann die spezifischen Inhalte, um die Berechtigungsstufen zu verwalten. Der Widerruf von Berechtigungen für einen Link deaktiviert in effizienter Weise diesen Link. Niemand wird danach in der Lage sein, diesen Link zu verwenden, um auf die Inhalte zuzugreifen, es sei denn, dass Sie sich dazu entscheiden, diesen Link erneut zu teilen.

Mit Microsoft OneDrive für Unternehmen verwaltete Dateien werden von solchen Dateien getrennt gespeichert, die in Ihrem persönlichen Microsoft OneDrive gespeichert sind. OneDrive for Business erhebt und überträgt Daten für die Authentifizierung, z. B. Ihre E-Mail-Adresse und Ihr Kennwort, die an Microsoft und/oder an den Anbieter Ihres Office 365-Dienstes übertragen werden.

Outlook

Outlook-Produkte sind dafür entwickelt, Ihre Produktivität durch eine bessere Kommunikation zu optimieren und umfassen Outlook.com, Outlook-Apps und andere damit verbundene Dienste.

Outlook.com. Outlook.com ist der primäre E-Mail-Dienst von Microsoft für Verbraucher und umfasst E-Mail-Konten mit Adressen, die auf outlook.com, live.com, hotmail.com und msn.com enden. Outlook.com bietet Funktionen, mit

denen Sie sich mit Ihren Freunden über soziale Netzwerke verbinden können. Sie müssen ein [Microsoft-Konto](#) erstellen, um Outlook.com zu verwenden.

Wenn Sie eine E-Mail oder ein Element aus einem Postfach in Outlook.com löschen, wird das Element in der Regel in den Ordner „Gelöschte Objekte“ verschoben, wo es für ca. 7 Tage verbleibt, es sei denn, dass Sie es zurück in Ihren Posteingang verschieben, Sie den betreffenden Ordner leeren oder der Dienst den Ordner automatisch leert, je nachdem, was zuerst eintritt. Sobald der Ordner „Gelöschte Objekte“ geleert wurde, verbleiben die gelöschten Objekte für 30 Tage in unserem System und werden danach endgültig gelöscht.

Outlook-Apps. Outlook-Client-Apps sind Software, die Sie auf Ihrem Gerät installieren und mit denen Sie E-Mail, Kalendereinträge, Dateien, Kontakte und andere E-Mail-Daten sowie Ihren Dateispeicher und andere Dienste, wie Exchange Online, Outlook.com oder Server, wie Microsoft Exchange, verwalten. Mit Outlook-Apps können Sie mehrere Konten von verschiedenen Anbietern, inklusive Drittanbietern, verwalten.

Um ein Konto hinzuzufügen, müssen Sie Outlook die Berechtigung für den Zugriff auf Daten aus E-Mail oder Dateispeicherdiensten erteilen.

Wenn Sie Outlook ein Konto hinzufügen, werden Ihre E-Mail-Nachrichten, Kalendereinträge, Dateien, Kontakte, Einstellungen und andere Daten des Kontos mit Ihrem Gerät synchronisiert. Bei Verwendung der mobilen Outlook-Apps werden diese Daten ebenfalls mit Microsoft-Servern synchronisiert, um zusätzliche Funktionen zu aktivieren. Dazu gehören schnellere Suchergebnisse, personalisiertes Filtern weniger wichtiger E-Mails und die Möglichkeit, E-Mail-Anlagen von verknüpften Dateispeicheranbietern ohne Verlassen der Outlook-App hinzuzufügen. Bei der Verwendung der Desktop-Outlook-App können Sie auswählen, ob Ihre Daten mit unseren Servern synchronisiert werden sollen. Sie können jederzeit ein Konto entfernen oder die Daten ändern, die von Ihrem Konto synchronisiert werden.

Wenn Sie ein Unternehmenskonto (z. B. das Ihres Arbeitgebers oder Ihrer Schule) hinzufügen, kann der Besitzer der Organisationsdomäne Richtlinien und Regelungen implementieren (z. B. eine mehrstufige Authentifizierung oder die Möglichkeit, Daten aus der Ferne zu löschen), die sich auf die Nutzung von Outlook auswirken können.

Um mehr über die von Outlook erfassten und verwalteten Daten zu erfahren, lesen Sie den Abschnitt [Office](#) in diesen Datenschutzbestimmungen.

Skype

Mit Skype können Sie Sprach-, Video- und Sofortnachrichten senden und empfangen. Dieser Abschnitt gilt für die Verbraucherversion von Skype; wenn Sie Skype for Business verwenden können Sie im folgenden Abschnitt [Produkte für](#)

[Unternehmen und Entwickler](#) weitere Informationen über diese Datenschutzbestimmungen erfahren. Microsoft Corporation und Skype Communications S.à.r.l. (eine hundertprozentige Tochtergesellschaft von Microsoft mit Sitz in Luxemburg) sind die für die Verarbeitung Verantwortlichen für Skype, und Verweise auf Microsoft in diesem Abschnitt beziehen sich auf beide juristischen Personen.

Im Rahmen der Bereitstellung dieser Funktionen erhebt Microsoft Nutzungsdaten über Ihre Mitteilungen, welche Uhrzeit und Datum der Kommunikation und die Nummern oder Benutzernamen umfasst, die Teil der Kommunikation sind.

Skype-Profil. Damit andere Personen Sie in Skype (oder in Produkten, die mit Skype interagieren, z. B. Skype for Business) finden, wird Ihr Skype-Profil je nach Ihren Profileinstellungen im öffentlichen Skype-Suchverzeichnis aufgenommen. Ihr Profil enthält Ihren Benutzernamen, Avatar sowie alle anderen Daten, die Sie Ihrem Profil hinzufügen oder Dritten anzeigen.

Skype-Kontakte. Bei Verwendung eines Microsoft-Dienstes, wie z. B. Outlook.com, wird Skype automatisch Ihrer Skype-Kontaktliste bekannte Personen hinzufügen, bis Sie uns auffordern, damit aufzuhören. Mit Ihrem Einverständnis prüft Skype außerdem gelegentlich Ihr Gerät oder andere Adressbücher, um Ihre Freunde automatisch als Skype-Kontakte hinzuzufügen. Sie können Benutzer blockieren, deren Mitteilungen Sie nicht mehr erhalten möchten.

Partnerunternehmen. Damit noch mehr Menschen Zugang zu Skype haben, gehen wir Partnerschaften mit anderen Unternehmen ein, sodass Skype über die Dienste dieser Unternehmen angeboten werden kann. Wenn Sie Skype über ein anderes Unternehmen als Microsoft nutzen, unterliegt der Umgang mit Ihren Daten den Datenschutzrichtlinien dieses Unternehmens. Um geltendes Recht einzuhalten, auf Gerichtsverfahren zu reagieren oder unser Partnerunternehmen bzw. unseren lokalen Betreiber bei entsprechenden Vorgängen zu unterstützen, können wir auf Ihre Daten zugreifen, diese übertragen, weitergeben und aufbewahren. Diese Daten können z. B. private Inhalte wie Inhalte Ihrer Sofortnachrichten, gespeicherte Videonachrichten, Voicemails oder Dateiübertragungen enthalten.

Skype Manager. Mit Skype-Manager können Sie die Nutzung von Skype einer Gruppe (z. B. Ihrer Familie) zentral verwalten. Wenn Sie eine Gruppe einrichten, sind Sie der Skype-Manager-Administrator, und Sie sehen die Nutzungsmuster, einschließlich detaillierter Informationen wie z. B. Datenverkehrsdaten und die Details der Einkäufe von anderen Gruppenmitgliedern, die einem solchen Zugriff zugestimmt haben. Wenn Sie Informationen wie Ihren Namen hinzufügen, sind Sie für andere Benutzer in der Gruppe sichtbar. Gruppenmitglieder können die Zustimmung für Skype-Manager auf ihrer Kontoseite auf www.skype.com widerrufen.

Das Skype-Marketing-Partnerprogramm. Damit noch mehr Menschen von Skype erfahren, ermutigen wir andere Unternehmen und Organisationen, sich als

Marketing-Partner zu registrieren, um Kunden an Skype zu verweisen. Wenn diese weitergeleiteten Kunden bestimmte Vorgänge tätigen, z. B. Skype-Guthaben kaufen, werden die Partner dafür bezahlt. Wir arbeiten mit einem anderen Unternehmen, Conversant Media, zusammen, um unser Partnernetzwerk zu betreiben. Microsoft, unser Partnernetzwerk und unsere Marketing-Partner verwenden Cookies und Web-Beacons. Dadurch erfahren wir, welcher Marketing-Partner eine erfolgreiche Kundenempfehlung abgegeben und Anspruch auf eine Zahlung hat. Microsoft hat keinen Einfluss auf Cookies, die von Marketing-Partnern abgelegt werden. Weitere Informationen zu den Datenschutzrichtlinien unserer Netzwerkpartner finden Sie unter <http://www.conversantmedia.com/legal/privacy>.

Push-Benachrichtigungen. Skype-Apps verwenden den Benachrichtigungsdienst auf Ihrem Gerät, um Sie über eingehende Anrufe, Chats und andere Benachrichtigungen zu informieren. Diese Dienste werden bei vielen Geräten durch andere Unternehmen zur Verfügung gestellt. Skype muss mit dem Benachrichtigungsdienst kommunizieren, damit dieser Sie z. B. darüber informieren kann, wer anruft oder um Ihnen die ersten Worte eines neuen Chats zur Verfügung zu stellen. Das Unternehmen, das den Benachrichtigungsdienst auf Ihrem m Gerät bereitstellt, verwendet diese Informationen gemäß seinen eigenen Bestimmungen und Datenschutzrichtlinien. Microsoft übernimmt keine Verantwortung für die Daten, die vom Unternehmen erfasst werden, das den Benachrichtigungsdienst bereitstellt. Wenn Sie die Benachrichtigungsdienste für eingehende Skype-Anrufe und -Nachrichten nicht verwenden möchten, deaktivieren Sie sie in den Einstellungen der Skype-App oder Ihres Gerät.

Skype-Werbung. Bestimmte Skype-Software enthält interessenbezogene Werbung, sodass Sie mit höherer Wahrscheinlichkeit Werbung angezeigt bekommen, die Sie interessieren wird. In einigen Versionen der Software können Sie interessenbezogene Werbung über das Menü mit den Datenschutzoptionen oder Kontoeinstellungen ablehnen. Wenn Sie sich mit einem Microsoft-Konto bei Skype anmelden, können Sie interessenbezogene Werbung unter <http://choice.microsoft.com> ablehnen. Bei einer Ablehnung wird Ihnen in der Skype-Software weiterhin Werbung basierend auf dem Land Ihres Wohnsitzes, Ihrer bevorzugten Sprache und dem Standort Ihrer IP-Adresse angezeigt. Es werden aber keine weitere Daten zum Anpassen der Werbung verwendet.

Übersetzungsfunktionen. Damit Sie mit Menschen in verschiedenen Sprachen kommunizieren können, bieten einige Skype-Apps Features zur Übersetzung von Audio und/oder Text an. Bei der Nutzung von Übersetzungsfunktionen werden Ihre Sprach- und Textdaten dazu verwendet, die Spracherkennungs- und Übersetzungsdienste von Microsoft bereitzustellen und zu verbessern.

Aufzeichnungsfeature. Einige Versionen von Skype verfügen über ein Aufzeichnungsfeature, mit dem Sie Audio- und Videoclips Ihrer Kommunikation aufnehmen und teilen können. Wenn Sie eine Sitzung aufnehmen, kann die Aufzeichnung einige Sekunden des Anrufs aus dem Speicher vor dem Initiieren der Aufzeichnung enthalten. Die Aufzeichnung wird als Teil des Unterhaltungsverlaufs

und unter Umständen auch lokal auf Ihrem Gerät gespeichert. **Sie sollten Ihre rechtliche Verantwortung kennen, bevor Sie eine Kommunikation aufzeichnen. Dazu müssen Sie auch wissen, ob Sie im Vorhinein die Zustimmung aller an der Kommunikation beteiligten Parteien einholen müssen.** Microsoft ist nicht dafür verantwortlich, wie Sie Ihre Aufzeichnungsfunktionen oder Ihre Aufzeichnungen nutzen.

Suche und künstliche Intelligenz

Produkte für die Suche und künstliche Intelligenz liefern Ihnen Informationen und erahnen, verarbeiten und setzen auf intelligente Art und Weise Informationen um, indem Sie mit der Zeit lernen und sich anpassen.

Bing

Bing-Dienste umfassen Such- und Zuordnungsdienste sowie die Bing Toolbar und Bing Desktop-Apps. Bing-Dienste sind auch in anderen Microsoft-Diensten wie beispielsweise [MSN](#) Apps und [Cortana](#) sowie in bestimmten Features in [Windows](#) enthalten (diese werden als von Bing bereitgestellte Features bezeichnet).

Sobald Sie eine Suche durchführen oder ein von Bing bereitgestelltes Feature verwenden, die eine Suche oder die Eingabe eines Befehls Ihrerseits enthält, erfasst Microsoft die von Ihnen eingegebenen Such- bzw. Befehlsbegriffe zusammen mit Ihrer IP-Adresse, Ihrer Position, den in unseren [Cookies](#) enthaltenen eindeutigen IDs, der Uhrzeit und dem Datum Ihrer Suche sowie Ihrer Browserkonfiguration. Wenn Sie sprachfähige Dienste von Bing nutzen, werden Ihre Spracheingabe- und Leistungsdaten, die mit der Sprechfunktionalität in Verbindung stehen, an Microsoft gesendet werden. Wenn Sie von Bing bereitgestellte Features wie „Cortana fragen“ oder die Bing-Suche verwenden, um auf einer Webseite oder in einem Dokument nach einem Wort oder einer Phrase zu suchen, wird das Wort bzw. die Phrase zusammen mit dem zugehörigen Kontext an Bing gesendet, um für den Kontext relevante Suchergebnisse bereitzustellen.

Suchvorschläge. Bei dem Feature „Suchvorschläge“ werden die Zeichen, die Sie in ein Bing-Feature eingeben, um eine Suche durchzuführen, an Microsoft gesendet. So können wir Ihnen Anregungen anzubieten, während Sie Ihre Suchbegriffe eingeben. Unter [Bing-Einstellungen](#) können Sie dieses Feature während der Bing-Suche aktivieren bzw. deaktivieren. Suchvorschläge können in Cortana nicht deaktiviert werden. Unter Windows können Sie Cortana und das Suchfeld immer ausblenden, um das Feature nicht anzuzeigen.

Das Verbesserungsprogramm für die Nutzung von Bing für Bing Desktop und Bing Toolbar. Wenn Sie Bing Desktop oder die Bing Toolbar verwenden und am Verbesserungsprogramm für die Nutzung von Bing teilnehmen wollen, sammeln wir außerdem zusätzliche Informationen darüber, wie Sie diese speziellen Bing-Apps verwenden wie z. B. die Adressen der von Ihnen besuchten Webseiten, um die Such-Rangliste und -Relevanz zu verbessern. Um dabei zu helfen, Ihre

Privatsphäre zu schützen, verwenden wir die über das Verbesserungsprogramm für die Nutzung von Bing erfassten Informationen nicht für eine Identifizierung von Ihnen oder für eine Kontaktaufnahme mit Ihnen oder für eine auf Sie abzielende Werbung. Sie können das Verbesserungsprogramm für die Nutzung von Bing jederzeit in den Bing Desktop- oder Bing Toolbar-Einstellungen deaktivieren. Zu guter Letzt löschen wir die über das Verbesserungsprogramm für die Nutzung von Bing erfassten Informationen nach 18 Monaten.

Aufbewahrung und De-Identifizierung. Für Bing-Suchanfragen führen wir eine De-Identifizierung von gespeicherten Abfragen durch, indem die vollständige IP-Adresse nach 6 Monaten sowie Cookie-IDs und andere sitzungsübergreifende Identifizierungen nach 18 Monaten entfernt werden.

Die Personalisierung über ein Microsoft-Konto. Einige Bing-Dienste bieten Ihnen eine erweiterte Erfahrung an, sobald Sie sich mit Ihrem persönlichen [Microsoft-Konto](#) anmelden, beispielsweise das Synchronisieren Ihres Suchverlaufs auf allen Geräten. Sie können diese Personalisierungsfunktionen dazu verwenden, um Ihre Interessen, Favoriten und Einstellungen anzupassen und Ihr Konto mit Drittanbieter-Diensten zu verbinden. Besuchen Sie Seite [Bing-Einstellungen](#), um Ihre persönlichen Einstellungen oder das Microsoft-Datenschutz-Dashboard zu verwalten.

Das Verwalten des Suchverlaufs. Bings Suchverlaufsdienst bietet eine einfache Möglichkeit, die von Ihnen eingegebenen Suchbegriffe und angeklickten Resultate erneut zu besuchen, während Sie die Bing Suche in Ihrem Browser verwenden. Sie können den Suchverlauf im Microsoft-Datenschutz-Dashboard unter <https://account.microsoft.com/privacy> löschen. Durch das Löschen Ihres Verlaufs wird dieser aus dem Suchverlaufsdienst entfernt und nicht mehr auf der Webseite angezeigt, löscht aber keine Informationen von unseren Suchprotokollen, die wie oben beschrieben, beibehalten und de-identifiziert werden.

Nicht von Microsoft stammende Dienste, die Bing nutzen. Sie haben die Möglichkeit, auf Bing-Features zurückzugreifen, während Sie nicht von Microsoft stammende Dienste verwenden wie z. B. die von Yahoo! Um diese Dienste anzubieten, empfängt Bing suchbezogene Informationen von diesen und weiteren Partnern, die Datum, Uhrzeit, IP-Adresse, eine eindeutige Kennung und andere suchbezogene Daten enthalten können. Diese Daten werden an Microsoft gesendet, um den Suchdienst anbieten zu können. Microsoft wird diese Daten, wie in dieser Erklärung beschrieben, oder wie es sich aus unseren weiter beschränkten Vertragspflichten mit unseren Partnern ergibt, verwenden. Für alle Fragen bezüglich wie Daten gesammelt oder verwendet werden, beziehen Sie sich bitte auf die Datenschutzrichtlinien der nicht von Microsoft stammenden Dienste.

Die Suchanfrage wurde an die verweisende URL übergeben. Sobald Sie auf ein Suchergebnis oder auf eine Werbung aus einer Bing-Suchergebnisseite klicken und sich auf die Ziel-Webseite begeben, wird die Ziel-Webseite die Standarddaten erhalten, die Ihr Browser an jede von Ihnen besuchte Webseite sendet wie z. B. Ihre

IP-Adresse, Browser-Typ, Sprache und die URL der Webseite, auf der Sie waren (in diesem Fall ist dies die Bing-Suchergebnisseite). Da die URL der Bing-Suchergebnisseite den Text der von Ihnen eingegebenen Suchabfrage (die Namen, Adressen oder weitere identifizierbare Informationen enthalten kann) enthält, ist die Ziel-Webseite in der Lage, den von Ihnen eingegebenen Suchbegriff zu ermitteln.

Möglicherweise ist Ihr Browser dafür konfiguriert, Seiten im Hintergrund zu laden, um die Leistung zu verbessern. Wenn Ihr Browser eine Seite im Hintergrund lädt, entspricht dies einem Besuch auf dieser Seite, d. h., die URL der Suchergebnisseite von Bing (mit Ihrer Suchabfrage) wird gesendet und alle [Cookies](#) werden von dieser Seite heruntergeladen.

Das Freigeben von Suchdaten zu Forschungs- und Entwicklungszwecken. Für Forschungs- und Entwicklungszwecke teilen wir einige der de-identifizierten Suchergebnisdaten, inklusive Sprachabfragen, mit ausgewählten Drittanbietern. Zuvor werden jedoch alle eindeutigen Erkennungsmöglichkeiten wie IP-Adressen und Cookie-IDs von diesen Daten gelöscht. Darüber hinaus durchlaufen die Daten einen Prozess, bei dem bestimmte sensible Daten entfernt werden, die Nutzer möglicherweise selbst in die Suchbegriffe eingegeben haben (z. B. Sozialversicherungsnummern oder Kreditkartennummern). Außerdem hält Microsoft diese Drittanbieter dazu an, die Daten sicher zu speichern und nicht für andere Zwecke zu verwenden.

Cortana

Cortana ist Ihr persönlicher Assistent. Je nach den Funktionen des Geräts und der Version von Cortana, die Sie verwenden (Windows, Xbox oder iOS usw.), kann Cortana eine Reihe von Funktionen bereitstellen, von denen einige personalisiert sind. Cortana funktioniert am besten, wenn Sie sich anmelden und es Daten aus Ihrem Gerät, sowie aus Ihrem persönlichen Microsoft-Konto, Ihrem AAD-Konto und anderen Microsoft-Diensten und Drittanbieter-Diensten, die Sie auswählen, nutzen kann. Wenn Sie sich bei Windows-Geräten nicht bei Cortana anmelden möchten, können Sie sich trotzdem mit Cortana unterhalten und ihre Hilfe bei der Suche im Internet und nach E-Mails, Kontakten und Ihren Dokumenten nutzen auf Ihrem Gerät oder in Microsoft-Diensten wie OneDrive gespeichert sind. Im Unterabschnitt [Windows Search](#) finden Sie weitere Informationen. Wenn Sie sich nicht anmelden, sind Ihre Erfahrungen eingeschränkt und werden nicht personalisiert. In iOS-, Android-Geräten und anderen Cortana-Fähigen Geräten funktioniert Cortana nur nach Anmeldung.

Abgemeldet. Wenn Sie nicht auf einem Windows-Gerät angemeldet sind, erhebt Cortana Daten darüber, wie Sie mit Cortana sprechen und Cortana per Spracherkennung, Freihand und Eingabe zur Suche verwenden. Diese Daten enthalten Folgendes:

- **Spracherkennungsdienste.** Um Cortana dabei zu helfen, Ihre Sprechweise und Sprachbefehle besser zu verstehen, werden die Sprachdaten an Microsoft gesendet, um Sprachmodelle anzufertigen und die Spracherkennung, sowie das Verständnis des Anliegen der Benutzer zu verbessern. Wenn Sie sich anmelden, werden die Sprachmodelle weiter personalisiert.
- **Abfragen und Suchverlauf.** Ihre Bing-Suchabfragen und im Feature „Suchvorschläge“ werden – auch wenn Cortana diese für Sie sucht – wie jede andere Bing-Suchanfrage behandelt und werden wie im Abschnitt [Bing](#) beschrieben verwendet.
- **Gerätedaten.** Cortana kann auf Daten über Ihr Gerät und dazu, wie Sie es verwenden, zugreifen. Es ermittelt beispielsweise ob Bluetooth oder der Sperrbildschirm aktiviert sind, Ihre Alarmeinrichtungen und welche Apps Sie installieren und nutzen.

Angemeldet. Wenn Sie sich anmelden, kann Cortana zusätzliche Aufgaben ausführen und eine personalisierte Erfahrung und relevante Vorschläge bieten. Mit Ihrer Zustimmung erhebt und greift Cortana außerdem auf folgende zusätzliche Arten von Daten zu, von denen einige von den Funktionen der Version von Cortana, die Sie verwenden (z.B. Windows, Android, iOS usw.) und der verwendeten App oder dem Geräte, auf der Cortana integriert ist, abhängen (z.B. Skype):

- **Microsoft-Konto.** Cortana kann auf die von Ihnen bei der Erstellung Ihres persönlichen [Microsoft-Konto](#) angegebenen demografischen Daten (wie beispielsweise Alter, Postleitzahl und Geschlecht) zugreifen.
- **Verwendung anderer Microsoft-Produkte.** Cortana verwendet Daten, die über andere Microsoft-Dienste erfasst wurden, um personalisierte Vorschläge zu machen. Beispielsweise verwendet Cortana Daten, die durch die Sport-App erhoben wurden und kann so automatisch Informationen über die Mannschaften anzeigen, denen Sie folgen. Über die Microsoft-App „Karten“ erfährt Cortana auch Ihre Lieblingsorte, erkennt Ihre bevorzugten Songs und Künstler anhand der in [Groove-Musik](#) abgespielte Musik, was Sie sich ansehen und bei [Microsoft Store](#) kaufen, und kann Ihnen dadurch bessere Vorschläge anbieten. Ihre Interessen in Cortanas Notizbuch können von anderen Microsoft-Diensten wie Bing und MSN verwendet werden, um auch dort Ihre Interessen, Vorlieben und Favoriten anzupassen.

Position. Sie können wählen, ob Cortana auf Ihren aktuellen Standort zugreifen kann, um Ihnen die wichtigsten Hinweise und Ergebnisse anzuzeigen und um Anregungen zu geben, die Ihnen dabei helfen, Zeit zu sparen wie z.B. Verkehrsinformationen und Standort-basierte Erinnerungen. Wenn Sie Cortana die Berechtigung erteilen, erhebt und verwendet es regelmäßig Ihre aktuelle Position, Ihren Positionsverlauf und andere Positionssignale (wie Positionen, die auf Fotos angegeben sind, die Sie auf OneDrive hochladen). Von Cortana erhobene Standortinformationen können ebenfalls in einem anonymisierten Format verwendet werden, um die Windows-Positionsdienste zu verbessern. Weitere Informationen finden Sie im Unterabschnitt [Positionsdienste](#).

Kontakte, E-Mail, Kalender und Kommunikationen. Sie können den Zugriff von Cortana auf Ihre Gerät und Ihre Cloud-basierte E-Mail und andere Kommunikationen, Ihren Kalender und Ihre Kontakte auswählen, um zusätzliche Funktionen zu aktivieren und zu personalisieren. Wenn Sie die Berechtigung erteilen, greift Cortana auf zusätzliche Daten zu, einschließlich:

- **Kontakte, SMS und E-Mail.** Cortana greift auf Ihre Kontakte und Mitteilungen zu, um eine Vielzahl von Dingen zu tun, beispielsweise: Anrufe tätigen, wenn Cortana mit Skype verbunden ist, Ihnen zu ermöglichen, Ereignisse zu Ihrem Kalender hinzuzufügen, Sie über wichtige Mitteilungen oder Kontakte in Kenntnis zu setzen und Sie über Ereignisse oder andere Dinge auf dem Laufenden zu halten, die für Sie wichtig sind, wie beispielsweise die Nachverfolgung von Paketen, Engagements oder Flügen. Cortana verwendet Ihre Kontakte und Mitteilungen auch dafür, Sie bei der Planung rund um Ihre Veranstaltungen zu unterstützen und bietet weitere Anregungen und Empfehlungen.
- **Kommunikationsverlauf.** Cortana lernt aus dem Verlauf Ihrer Anrufe, SMS und E-Mails, wer für Sie am wichtigsten ist. Diese Daten dienen dazu, Kontakte zu verwalten, die am wichtigsten für Sie sind und Ihre bevorzugten Kommunikationsmethoden zu ermitteln, wichtige Nachrichten für Sie zu kennzeichnen (wie z. B. verpasste Anrufe) und die Leistungsfähigkeit der Funktionen von Cortana, beispielsweise die Spracherkennung, zu verbessern.
- **Termine im Kalender.** Cortana greift auf Ihren Kalender zu, um Sie an Termine zu erinnern und relevante Informationen darüber anzubieten.

Browserverlauf. Wenn Sie Cortana erlauben, Ihren vollständigen Browserverlauf zu verwenden, erfasst Microsoft Ihre Microsoft Edge-Suchanfragen und Ihren vollständigen Browser-Verlauf zusammen mit einer verknüpften Benutzer-ID. Cortana wird diese Daten verwenden, um Sie besser kennenzulernen und um Ihnen zeitnahe und intelligente Antworten und personalisierte Vorschläge anzubieten, oder Web-Aufgaben für Sie zu vervollständigen. Cortana sammelt keine Informationen zu Webseiten, die Sie auf InPrivate-Registerkarten besuchen.

Andere verbundene Dienste und Skills. Sie können Cortana auch den Zugriff auf andere, von Microsoft- und Drittanbieterdiensten gesammelte Daten erlauben oder diese Info mit den Diensten teilen, indem Sie Ihre Zugriffsberechtigung erteilen oder diese Dienste mit Cortana verbinden. Wenn Sie einen verbundenen Dienst oder Drittanbieter-Skills aktivieren, teilt Cortana Ihre Anfrage mit diesen Diensten oder Drittanbietern, um Ihren Befehl auszuführen. Cortana kann ebenfalls zusätzliche Informationen teilen, die Sie freigeben (z. B. Ihre Position). Alle Informationen, die Sie mit einem Drittanbieter bei der Verwendung von verbundenen Diensten oder Drittanbieter-Skills austauschen, unterliegen den Datenschutzbestimmungen und Nutzungsbedingungen des Drittanbieters. Cortana verwendet Ihre Abfragen und Antworten aus den Interaktionen mit verbundenen Dienste oder Drittanbieter-Skills zur Verbesserung der Spracherkennung und Sprechweise, um Ihnen und personalisierte Vorschläge und Features vorzuschlagen.

Im folgenden finden Sie Beispiele für verbundene Dienste und Skills. Neue verbundene Dienste und Skills werden regelmäßig hinzugefügt.

- **Verbundene Microsoft-Dienste.** Wenn Sie Cortana mit Ihrem [Xbox Live](#)-Konto verbinden, kann es auf Ihre Xbox Live-Daten zugreifen und mehr über Ihre Spielaktivitäten erfahren, Ihnen daraufhin relevante Inhalte und Vorschläge unterbreiten, Sie darüber benachrichtigen, wenn Freunde spielbereit sind und Ihnen bei der Planung Ihrer Spielsitzungen helfen. Wenn Sie Cortana mit Ihrem [Office 365](#) Geschäfts- oder Schulkonto verbinden, kann es auf die in Office 365 gespeicherten Daten zugreifen, um Sie auf dem Laufenden zu halten und Einblicke in Ihre Besprechungen, Dokumente und Beziehungen zu erhalten. Es ist Microsoft möglich, durch Ihre Anmeldung innerhalb Cortanas in LinkedIn, auf bestimmte LinkedIn-Daten zuzugreifen, so dass Cortana Ihnen besser personalisierte Informationen und Empfehlungen liefern können. Cortana sendet erlaubt LinkedIn den Zugriff auf Namen, E-Mail-Adressen, Titel und Firmennamen von Personen, mit denen Sie Termine haben, damit es die relevanten Informationen über diese Kontakte abrufen kann.
- **Andere verbundene Dienste und Skills.** Sie können mithilfe von Cortana auf Dienste von Drittanbieter zugreifen, um zusätzliche Hilfe und personalisierte Erfahrungen, basierend auf den Daten der Drittanbieterdienste zu erhalten. Nicht alle Skills erfordern eine Authentifizierung. Mit Ihrem Einverständnis kann **Cortana ebenfalls Informationen über Sie und Ihre Anfrage an einen Drittanbieter senden.** Auf ähnliche Weise sendet Cortana Ihre aktuelle Position und Ihren Zielort an Uber, wenn Sie über Cortana einen Wagen bestellen. Verwalten Sie die verbundenen Dienste und Skills von Cortana im Notizbuch von Cortana.

Wenn Sie Cortana Zugriff auf Ihre Daten von einem Gerät oder Dienst erteilen, kann diese Informationen verwendet werden, um Cortana auf jedem Gerät oder Dienst, auf dem Sie Cortana aktiviert haben, zu personalisieren. Sie können sich jederzeit bei Cortana abmelden. Wenn Sie sich bei Windows abmelden, steht Ihnen der Service auch dann noch zur Verfügung, allerdings wird Ihre Erfahrung nicht mehr personalisiert. Sie können die Art der Daten, die Cortana verwendet und was es über Sie erfährt in den Cortana-Einstellungen, -Berechtigungen und im -Notizbuch verwalten. Weitere Informationen zu den einzelnen Features und zu deren Verwaltung finden Sie unter <http://go.microsoft.com/fwlink/?linkid=522360>.

Microsoft Translator

Microsoft Translator ist ein statistisches Übersetzungssystem für die automatische Übersetzung von geschriebenem und gesprochenem Text in zahlreiche Sprachen. Translator kann in andere Microsoft-Produkte und Dienste wie Office, SharePoint und Bing integriert werden. Drittanbieter können Translator auch in ihre eigenen Dienste und Angebote integrieren. Informationen über den Datenschutz bei

Diensten und Angeboten von Drittanbietern finden Sie in deren Datenschutzrichtlinien.

Microsoft Translator sammelt und verwendet die von Ihnen übermittelten Text-, Bild- und Sprachdaten sowie Informationen über den Zugriff auf den Translator-Dienst, also Daten wie beispielsweise Betriebssystemversion, Browsertyp und Sprache. Wir verwenden Ihre Daten, um den Translator-Dienst anzubieten und um Ihre Erfahrung mit dem Dienst zu verbessern und zu personalisieren. Microsoft hat geschäftliche und technische Maßnahmen implementiert, die dazu dienen, Translator-Daten unkenntlich zu machen. Zum Beispiel verwenden wir zur Verbesserung von „Übersetzer“ zufällige Texte, und wir löschen darin alle Zeichenfolgen und persönliche Informationen, die zur Identifizierung dienen können.

Wenn Sie die Microsoft Translator-API mit einem monatlichen Volumen von 250 Millionen Zeichen oder mehr abonnieren, können Sie anfordern, dass die Protokollierung für den Text, den Sie an Microsoft Translator senden, deaktiviert wird. Einzelheiten dazu finden Sie unter <https://www.microsoft.com/de-de/translator/notrace.aspx>.

SwiftKey

Die SwiftKey-Tastatur und ähnliche Apps und Dienste erfassen Daten über den eingegebenen Text - inklusive von Ihnen verwendete Emojis und wichtige Wörter - um Ihren Schreibstil zu lernen und eine personalisierte und Ihnen angepasste Autokorrektur und Texterkennung anzubieten.

Wenn Sie unsere Produkte verwenden, erfassen wir z. B. Geräte-, Netzwerk-, Leistungs- und Verwendungsstatistikdaten. Wir nutzen die erfassten Daten für den Betrieb und die Verbesserung unserer Produkte.

Wenn Sie SwiftKey Cloud verwenden, wird Ihre E-Mail-Adresse, grundlegende demografischen Daten und Daten über die von Ihnen verwendeten Wörter und Sätze erfasst, um Dienste wie Personalisierung, Synchronisierungsvorhersage und Datensicherung zu aktivieren. Durch die Art und Weise, wie Sie Sprache verwenden, lernt unsere Vorhersagetechnologie und kann so ein personalisiertes Sprachmodell erstellen. Dieses Modell ist eine optimierte Sicht über die von Ihnen am häufigsten verwendete Wörter und Sätze und spiegelt dadurch Ihren einzigartigen Stil wider. Zu diesem Zweck greift auf die SwiftKey-Tastatur für Android bei der ersten Installation auf Ihr SMS-Nachrichten zu. Der SwiftKey-Personalisierungsdienst ist eine Feature von SwiftKey Cloud und greift ebenfalls auf den zuletzt verwendeten Inhalt Ihrer angegebenen Onlinedienste, wie Gmail, Facebook und Twitter zu. Wenn Sie in der SwiftKey Cloud angemeldet sind, werden diese Daten über verschlüsselte Kanäle auf unsere Server übertragen. Die von einer Webseite oder App gekennzeichneten Daten der Felder für Kennwörter oder Zahlungsdaten werden von SwiftKey nicht protokolliert, gespeichert oder verwendet.

Wenn Sie nicht bei SwiftKey Cloud angemeldet sind, werden von Ihrem Gerät keine Einblicke in Ihre Sprachgewohnheiten erfasst. Sie können Ihre Einwilligung für unsere Verwendung und Aufbewahrung von persönlichen, von SwiftKey erfassten Daten, jederzeit im Abschnitt „SwiftKey Cloud“ unter „Einstellungen für SwiftKey“ widerrufen. Durch Widerrufen der Einwilligung werden Ihre persönlichen und durch die Verwendung der SwiftKey-Tastatur erfassten Daten gelöscht.

Möglicherweise erhalten Sie ab und zu Benachrichtigungen auf Ihrem Gerät über Produkt-Updates und Features, die für Sie von Interesse sein könnten. Sie können diese Benachrichtigungen in unseren Produkten jederzeit durch das Aufrufen der SwiftKey-Einstellungen deaktivieren.

Windows

Windows ist eine personalisierte Computer-Umgebung, die Sie zu einem nahtlosen Roaming und Zugang zu Diensten, Vorlieben und Inhalten über all Ihre IT-Geräte hinweg befähigt, von Handys über Tablets bis hin zu Surface Hubs. Anstatt als statisches Software-Programm auf Ihrem Gerät installiert, basieren die Schlüsselkomponenten von Windows auf Cloud und beide, sowohl Cloud als auch lokale Elemente von Windows werden regelmäßig aktualisiert, um Ihnen die neuesten Verbesserungen und Features zu bieten. Um dieses Computer-Erlebnis anzubieten, erheben wir Daten über Sie, Ihr Gerät und wie Sie Windows verwenden. Und weil Windows für Sie persönlich ist, geben wir Ihnen die Wahlmöglichkeiten darüber, welche persönlichen Daten wir erheben und wie wir diese verwenden. Beachten Sie, dass für den Fall, dass Ihr Windows-Gerät von Ihrer Organisation (wie Ihrem Arbeitgeber oder Ihrer Schule) verwaltet wird, Ihre Organisation zentrale Verwaltungstools verwenden kann, die von Microsoft oder anderen für die Kontrolle der Geräteeinstellungen, Geräterichtlinien, Software-Aktualisierungen, Datenerfassung durch uns oder die Organisation oder für andere Aspekte Ihres Geräts zur Verfügung gestellt werden. Weitere Informationen zur Datensammlung und zum Datenschutz in Windows finden Sie unter go.microsoft.com/fwlink/?LinkId=529552. Für ältere Versionen von Windows (einschließlich Vista, 7, 8 und 8.1) gelten eigene Datenschutzerklärungen.

Aktivierung

Sobald Sie Windows aktivieren, wird ein spezifischer Product Key mit dem Gerät verbunden, auf dem die Software installiert ist. Der Product Key, sowie Daten über die Software und Gerätetyp werden an Microsoft gesendet, um die Lizenz für die Software zu bestätigen. Diese Daten können erneut gesendet werden, falls sich eine Notwendigkeit ergibt, Ihre Lizenz erneut zu aktivieren oder zu validieren. Bei mit Windows betriebenen Telefonen werden auch die Geräte- und Netzwerkbezeichner sowie der Gerätestandort zum Zeitpunkt des erstmaligen Einschaltens des Gerätes für die Zwecke der Registrierung der Garantie, der Vorratsergänzung und der Betrugsprävention an Microsoft gesendet.

Werbe-ID

Windows generiert für jeden Benutzer eines Gerätes eine unverwechselbare Werbe-ID. Wenn die Werbe-ID aktiviert ist, können Apps (sowohl Microsoft- und Drittanbieter-Apps) auf diese zugreifen und sie auf ähnliche Weise wie Webseiten verwenden, die auf eine eindeutige, in einem Cookie gespeicherte Kennung, zugreifen. Daher kann Ihre Werbe-ID von App-Entwicklern und den mit ihnen verbundenen Werbenetzwerken verwendet werden, um eine mehr relevante Werbung und andere personalisierte Erfahrungen mit deren Apps und im Web anzubieten. Microsoft sammelt die Werbe-ID für die hier beschriebenen Nutzen nur dann, wenn Sie die Werbe-ID als Teil der Datenschutzeinstellung aktivieren. Sie können den Zugriff auf diese ID jederzeit deaktivieren, indem Sie die Werbe-ID in Ihren Datenschutzeinstellungen (unter Start > Einstellungen > Datenschutz) deaktivieren. Sobald Sie diesen erneut aktivieren, wird die Werbe-ID zurückgesetzt und eine neue Kennung erzeugt. Wenn eine Drittanbieter-App auf die Werbe-ID zugreift, unterliegt die Verwendung der Werbe-ID deren eigenen Datenschutzrichtlinien. Weitere Informationen dazu, wie Microsoft Daten zu Werbezwecken nutzt, finden Sie im Abschnitt [Wie wir Daten nutzen](#) in diesen Bestimmungen.

Diagnose

Wenn Sie Windows verwenden, erfassen wir Diagnosedaten, die uns dabei helfen, Probleme zu beheben und die Microsoft-Produkte zu verbessern. Wenn Sie die Option für **personalisierte Benutzererfahrung** aktivieren, können diese Daten auch zur Personalisierung von Microsoft-Produkten verwendet werden. Diese Daten werden mit mindestens einer eindeutigen Kennung versehen, an Microsoft gesendet und gespeichert. Sie helfen uns dabei, einen einzelnen Benutzer auf einem bestimmten Gerät zu erkennen, Servicefälle des Gerätes zu verstehen und Nutzungsmuster zu speichern. Es gibt drei Ebenen von Diagnose- und Nutzungsdaten: **Allgemein** und **Vollständig, Erweitert**. Auf der untersten Ebene **Allgemein** erfassen wir nur Daten, die erforderlich sind, um Windows-Geräte sicher und auf dem neuesten Stand zu halten. Allgemeine Daten umfassen Daten über das Gerät selbst sowie über die ordnungsgemäße Funktion von Updates für Windows und Microsoft Store. Hinzu kommen allgemeine Fehlerdaten. Bei der Einstellung „Allgemein“ werden folgende Daten erfasst:

- Geräte-, Verbindungs- und Konfigurationsdaten:
 - Daten über das Gerät wie Prozessortyp, OEM-Hersteller, Akku und Akkukapazität, Anzahl und Typ von Kameras, Firmware und Speicherattribute.
 - Netzwerkfunktionen und Verbindungsdaten wie die IP-Adresse des Geräts, mobiles Netzwerk (einschließlich IMEI und Mobilfunkanbieter) und ob das Gerät mit einem kostenlosen oder kostenpflichtigen Netzwerk verbunden ist.
 - Daten über das Betriebssystem und dessen Konfiguration wie Version und Build-Nummer des Betriebssystems; Region und

- Spracheinstellungen; Diagnoseebene; Angabe darüber, ob das Gerät Teil des Windows-Insider-Programms ist.
- Daten über verbundene Peripheriegeräte wie Modell, Hersteller, Treiber und Kompatibilitätswinformationen.
 - Daten über die Anwendungen, die auf dem Gerät installiert sind, beispielsweise Name, Version und Herausgeber der Anwendung.
 - Angaben darüber, ob ein Gerät für ein Update verfügbar ist oder ob Gründe vorliegen, die den Empfang von Updates verhindern können (beispielsweise niedriger Akkustand, wenig Festplattenspeicher oder Konnektivität über ein kostenpflichtiges Netzwerk).
 - Angaben darüber, ob Updates erfolgreich abgeschlossen wurden oder ob Fehler aufgetreten sind.
 - Daten über die Zuverlässigkeit des Diagnosesystems selbst.
 - Einfache Fehlerdaten wie Angaben über die Integrität von Betriebssystem und Anwendungen, die momentan ausgeführt werden. Beispielsweise wird bei dieser einfachen Fehlerberichterstattung übermittelt, ob eine Anwendung (z. B. Microsoft Paint) oder ein Spiel von Drittanbietern eingefroren oder abgestürzt ist.

Um zu erfahren, was für Daten vom Typ „Allgemein“ gesammelt wird, klicken Sie auf [Hier](#) (nur in englischer Sprache).

„Vollständig“ bedeutet: Es werden die bei der Einstellung „Allgemein“ erfassten Daten übermittelt sowie zusätzliche Informationen, die Microsoft verwendet, um Produkte und Dienste für alle Benutzer zu verbessern oder um Fehler zu beheben. Bei der Einstellung „Vollständig“ erfassen wir folgende zusätzliche Informationen:

- Daten zu Gerät, Konnektivität und Konfiguration (in größerem Umfang als bei der Einstellung „Allgemein“).
- Statusdaten und Protokolldaten über die Integrität des Betriebssystems und anderer Komponenten (zusätzlich zu den Daten über die Aktualisierungs- und Diagnose-Systeme, die bei der Einstellung „Allgemein“ erfasst werden).
- Daten über App-Verwendung – welche Programme werden auf einem Gerät gestartet, wie lange werden sie ausgeführt und wie schnell reagieren sie auf Eingaben.
- Browserverwendung, einschließlich dem Browserverlauf und Suchbegriffen auf Microsoft-Browsern, z. B. Microsoft Edge oder Internet Explorer.
- Kleine Beispiele für Freihand- und Tastatureingaben – aus ihnen werden alle Bezeichner, Sequenzierungsinformationen und andere Daten entfernt (z. B. Namen, E-Mail-Adressen und numerische Werte), die geeignet sind, den ursprünglichen Inhalt zu rekonstruieren oder die Eingabe dem Benutzer zuzuordnen. Diese Daten werden niemals verwendet, um die Benutzererfahrung zu personalisieren (wie unten beschrieben).
- Erweiterte Fehlerberichterstattung, die den Speicherstatus des Geräts bei einem System- oder App-Absturz umfasst. Dabei können unbeabsichtigt Anwenderdaten, wie beispielsweise Teile der Datei übermittelt werden, die Sie beim Auftreten des Problems verwendet haben. Absturzdaten werden

niemals verwendet, um die Benutzererfahrung zu personalisieren (wie unten beschrieben).

Wir stellen Partnern (z. B. OEMs) begrenzte Teile aus Fehlerberichten zur Verfügung, damit unsere Partner Probleme mit Produkten und Diensten beheben können, die mit Windows und anderen Produkten und Diensten von Microsoft in Zusammenhang stehen. Die Partner dürfen diese Daten ausschließlich zur Problembeseitigung oder Weiterentwicklung der genannten Produkte und Dienste verwenden.

Wenn Sie **personalisierte Benutzererfahrung** aktivieren, verwenden wir einige der oben unter „Diagnose“ beschriebenen Nutzungsdaten, um Ihre Erfahrung mit Windows und anderen Produkten und Diensten zu personalisieren. Dazu gehören Vorschläge zum Anpassen und Optimieren von Windows sowie Empfehlungen und Angebote über Windows-Funktionen und unterstützte Apps, Dienste, Hardware und Peripheriegeräte. Der Datenumfang hängt von Ihrer gewählten Diagnoseeinstellung ab – „Allgemein“ oder „Vollständig“. Wenn Sie die z. B. „Vollständig“ auswählen, enthalten Ihre Daten Informationen über die Browser- und App-Nutzung. Wenn Sie maßgeschneiderte Funktionen aktivieren, werden Ihre Absturzdaten, Freihand- oder Eingabedaten trotzdem nicht verwendet.

Positionsdienste & Motion Sensing & Aufzeichnung

Windows-Positionsdienst. Microsoft verfügt über einen Positionsdienst, welcher dabei hilft, die genaue geografische Position eines bestimmten Windows-Geräts zu bestimmen. Abhängig von den Fähigkeiten des Geräts wird der Standort durch den Satellitenpositionierungsdienst (GPS) bestimmt, welcher Mobilfunkmasten in der Nähe und/oder WLAN-Zugangspunkte erfasst und diese Informationen mit einer Datenbank vergleicht, die Microsoft für Mobilfunkmasten und WLAN-Zugangspunkte betreibt, deren Position bekannt ist oder die Ortung Ihrer IP-Adresse ableitet. Wenn der Ortungsdienst auf einem Windows-Gerät aktiviert ist oder Sie Microsoft-Apps erlauben, Positionsinformationen auf anderen Geräten zu erfassen, werden die Daten über Mobilfunkmasten und WLAN-Zugangspunkte sowie deren Standorte von Microsoft erhoben und der Positionsdatenbank hinzugefügt, nachdem alle Daten, welche die Person oder das Gerät identifizieren können vorher entfernt wurden. Microsoft kann diese de-identifizierte Positionsdaten auch Drittanbietern zur Verfügung stellen, um den Ortungs- und Kartendienst anzubieten und zu verbessern.

Windows-Dienste und Funktionen (wie Browser und Cortana), Apps, die unter Windows laufen und Webseiten, die in Windows-Browsern geöffnet werden, haben Zugang zum Windows-Ortungsdienst, um den genauen Standort zu bestimmen, falls Sie es ihnen ermöglichen, dies zu tun. Wenn Sie das erste Mal Windows installieren, erfordern einige Funktionen und Apps Ihre Erlaubnis für die genaue Standortbestimmung, wobei Sie bei einigen Apps jedes Mal und bei anderen Apps immer dann, wenn Sie den Ortungsdienst benutzen, um Erlaubnis gefragt werden.

Weitere Informationen zu bestimmten Windows-Apps, die den Positionsdienst verwenden, finden Sie im Abschnitt [Windows Apps](#) weiter unten.

Wenn Sie den Positionsdienst nutzen wird Ihr Windows-Gerät seine Position an Microsoft weitergeben und wir behalten nur den letzten bekannten Aufenthaltsort (jeder neue Aufenthaltsort ersetzt den vorherigen), um die Effizienz und Funktionen unserer Dienste zu verbessern. Die Daten über den aktuellen Positionsverlauf eines Windows-Geräts werden auf dem Gerät gespeichert, und bestimmte App- und Windows-Funktionen können auf diesen Positionsverlauf zugreifen. Sie können den Positionsverlauf des Geräts jederzeit im Einstellungsmenü des Geräts löschen.

In den Einstellungen können Sie auch sehen, welche Apps Zugriff auf den Positionsdienst oder den Positionsverlauf des Geräts haben, den Zugriff auf den Positionsdienst für bestimmte Anwendungen aktivieren bzw. deaktivieren oder den Positionsdienst ausschalten. Sie können ebenfalls den Standardstandort einstellen, wenn der Positionsdienst keine genauere Position für Ihr Gerät erkennen kann.

Beachten Sie, dass bei mobilen Geräten Ihr Mobilfunkanbieter Zugriff auf Ihre Position hat, auch wenn Sie den Positionsdienst für das Gerät deaktivieren.

Ungefährer Standort. Wenn Sie die ungefähre Standortfunktion aktivieren, haben Apps, die Ihre genaue Standortposition nicht verwenden, Zugriff auf Ihre ungefähre Standortposition, wie z. B. Ihre Stadt, Postleitzahl oder Region.

Mein Handy finden. Mit dem Feature „Mein Handy finden“ können Sie die Position Ihres Windows Phone über account.microsoft.com ermitteln, selbst wenn Sie jeglichen Zugriff auf den Positionsdienst auf dem Handy deaktiviert haben. Wenn Sie die Funktion „Meine Position alle paar Stunden speichern“ in den Einstellungen von „Mein Handy finden“ auf Ihrem Smartphone aktiviert haben, wird der zuletzt bekannte Standort Ihres Smartphones in regelmäßigen Abständen gesendet und gespeichert, auch wenn Sie den Positionsdienst des Smartphones ausgeschaltet haben. Jedes Mal, wenn ein neuer Standort gesendet wird, ersetzt dieser den zuvor gespeicherten Standort.

Mein Gerät suchen. Das Feature „Mein Gerät finden“ ermöglicht einem Administrator eines Windows-PCs oder Tablets, die Position des jeweiligen Gerätes zu finden, falls der Administrator den Positionsdienst für das Gerät aktiviert hat. Das gilt auch dann, wenn andere Benutzer die Position für sich selbst deaktiviert haben. Wenn der Administrator versucht, das Gerät zu finden, werden die Benutzer eine Benachrichtigung im Benachrichtigungszentrum sehen.

Windows-Bewegungssensor. Windows-Geräte mit Bewegungsaktivitätserkennung können Daten über die Bewegungsaktivität erfassen. Diese Daten befähigen Funktionen wie die eines Schrittzählers, der die Anzahl der von Ihnen getätigten Schritte zählt, so dass eine Fitness-App berechnen kann, wie viele Kalorien Sie verbrauchen. Diese Daten und ihr Verlauf werden auf Ihrem Gerät gespeichert und Apps, denen Sie die Berechtigung für den Zugriff und das Verwenden dieser Daten erteilen, können auf diese zugreifen.

„Aufnahme“. Einige Windows-Geräte besitzen auch eine Aufzeichnungsfunktion, die Ihnen die Erfassung von Audio- und Videoclips über Ihre Aktivitäten auf dem Gerät erlaubt, einschließlich der Kommunikation mit anderen. Wenn Sie sich dafür entscheiden, eine Sitzung aufzuzeichnen, wird die Aufzeichnung lokal auf Ihrem Gerät gespeichert. In einigen Fällen haben Sie die Option zum Senden der Aufzeichnung an ein Microsoft-Produkt oder -Dienst, der die Aufzeichnung öffentlich überträgt. **WICHTIG: Sie sollten Ihre rechtliche Verantwortung kennen, bevor Sie eine Kommunikation aufzeichnen und/oder übertragen. Dazu müssen Sie auch wissen, ob Sie im Vorhinein die Zustimmung aller an der Kommunikation beteiligten Parteien einholen müssen.** Microsoft ist nicht dafür verantwortlich, wie Sie Ihre Aufzeichnungsfunktionen oder Ihre Aufzeichnungen nutzen.

Sicherheitsfunktionen

Geräteverschlüsselung. Die Geräteverschlüsselung hilft dabei, die auf dem Gerät gespeicherten Daten durch eine Verschlüsselung mittels BitLocker Drive-Verschlüsselungstechnologie zu schützen. Wenn die Geräteverschlüsselung aktiviert ist, verschlüsselt Windows das Laufwerk auf dem Windows installiert ist automatisch und erstellt einen Wiederherstellungsschlüssel. Der BitLocker-Wiederherstellungsschlüssel für Ihr persönliches Gerät wird automatisch in Ihrem persönlichen Microsoft OneDrive-Konto online gesichert. Microsoft verwendet Ihre individuellen Wiederherstellungsschlüssel zu keinen anderen Zwecken.

Tool zum Entfernen bösartiger Software. Das Tool zum Entfernen bösartiger Software (MSRT) wird als Bestandteil von Windows Update mindestens einmal im Monat auf Ihrem Gerät ausgeführt. MSRT überprüft Geräte auf Infektionen durch bestimmte, weitverbreitete Schadsoftware („Malware“) und hilft, alle gefundenen Infektionen zu entfernen. MSRT bei Ausführung die auf der Microsoft Support-Webseite gelistete Malware entfernen, sollte sie sich auf Ihrem Gerät befinden. Während einer Malware-Überprüfung wird ein Bericht mit spezifischen Daten über die erkannte Malware, die Fehler und andere Daten über Ihr Gerät an Microsoft gesendet. Wenn Sie nicht möchten, dass das MSRT diese Daten an Microsoft sendet, können Sie die Berichtskomponente des MSRT deaktivieren.

Microsoft Family. Eltern können Microsoft Family verwenden, um den Gebrauch des Gerätes durch ihr Kind einzuschränken. Es stehen viele Features für Familienmitglieder zur Verfügung, weshalb Sie sich bitte die zur Verfügung gestellten Informationen durchlesen, bevor Sie eine Familie erstellen oder einer bestehenden Familie beitreten. Wenn die Berichterstattung über die Aktivität der Familie für ein Kind aktiviert wurde, wird Microsoft Einzelheiten dazu erheben, wie das Kind das Gerät verwendet und die Eltern mit Berichten über die Aktivitäten dieser Verwendung versorgen. Die Tätigkeitsberichte werden nach kurzer Zeit routinemäßig von den Microsoft-Servern gelöscht.

Windows Defender SmartScreen. Windows Defender SmartScreen hilft dabei, Sie bei der Nutzung unserer Dienste zu schützen, indem es heruntergeladene Dateien

und Webinhalte auf schadhafte Software, potenziell unsichere Webinhalte und andere Bedrohungen für Sie oder Ihr Gerät überprüft. Bei der Überprüfung einer Datei werden Daten zu dieser Datei an Microsoft gesendet, einschließlich des Dateinamens, des Downloadspeicherorts, eines Teils der Inhalte der Datei und der digitalen Zertifikate dieser Datei. Wenn Windows Defender SmartScreen die Datei als unbekannt oder potenziell unsicher identifiziert, dann erhalten Sie vor dem Öffnen der Datei eine Warnung. Während einer Überprüfung der Web-Inhalte werden die Daten über den Inhalt und Ihr Gerät, inklusive der vollständigen Web-Adresse des Inhalts an Microsoft gesendet. Sobald Windows Defender SmartScreen feststellt, dass der Inhalt möglicherweise nicht sicher ist, wird eine Warnung anstelle des Inhalts angezeigt. Windows Defender SmartScreen kann in den Einstellungen ein- oder ausgeschaltet werden.

Windows Defender Antivirus. Windows Defender Antivirus sucht nach Schadsoftware und nach weiterer unerwünschter Software auf Ihrem Gerät. Windows Defender Antivirus wird zum Schutz Ihres Gerätes automatisch aktiviert, sollte keine andere Antischadsoftware für den Schutz Ihres Gerätes aktiviert sein. Wenn Windows Defender Antivirus aktiviert ist, wird der Sicherheitsstatus Ihres Gerätes überwacht. Sobald Windows Defender Antivirus aktiviert ist oder durch die Funktion „Limitiertes regelmäßiges Scannen“ ausgeführt wird, wird er den Sicherheitsstatus Ihres Gerätes überwachen und automatisch Berichte an Microsoft senden, die Daten über vermutete Schadsoftware und weitere unerwünschte Software enthalten. Es werden auch Dateien gesendet, die Schadsoftware enthalten. Wenn ein Bericht mit hinreichender Wahrscheinlichkeit persönliche Daten enthält, dann wird dieser nicht automatisch gesendet. Ein entsprechender Hinweis wird vor dem Versenden angezeigt. Sie können Windows Defender Antivirus so konfigurieren, dass keinerlei Berichte und vermutete Schadsoftware an Microsoft gesendet werden.

Sprach-, Freihand- und Tastatureingabe

Windows bietet eine gerätebasierte Spracherkennungsfunktion (über die Desktop-App Windows-Spracherkennung) und einen cloudbasierten Spracherkennungsdienst, der zusammen mit Cortana in den Märkten und Regionen eingeführt wurde, in denen Cortana verfügbar ist. Um zu ermitteln, welche Sprachen und Regionen die Spracherkennung derzeit unterstützt, suchen Sie nach <https://support.microsoft.com/instantanswers/557b5e0e-0eb0-44db-87d6-5e5db6f9c5b0/cortana-s-regions-and-languages>. Bei der Verwendung von Cloud-basierter Spracherkennung sammelt und verwendet Microsoft Ihre Stimme, um Ihnen die Spracherkennung in Cortana und in anderen unterstützten Apps bereitzustellen.

Darüber hinaus werden Ihre getippten und handgeschriebenen Worte erhoben, um Ihnen ein personalisiertes Benutzerwörterbuch anzubieten, das Ihnen dabei hilft, mit einer besseren Zeichenerkennung auf Ihrem Gerät zu tippen oder zu schreiben, um Sie während des Tippens oder Schreibens mit Textvorschlägen zu versorgen.

Das Tippen von Daten enthält eine Stichprobe von Buchstaben und Wörtern, die Sie tippen, die wir bearbeiten, um IDs, IP-Adressen und andere potenzielle Identifikationsmöglichkeiten zu entfernen. Darin enthalten sind auch zugehörige Leistungsdaten, wie z. B. Textänderungen, die Sie manuell vornehmen, sowie Wörter, die Sie dem Wörterbuch hinzugefügt haben.

Als Teil des cloudbasierten Spracherkennungsdiensts erfassen wir auch Informationen aus dem auf Ihrem Gerät erstellten Benutzerwörterbuch. Sowohl die Stimmdateien als auch das Benutzerwörterbuch werden erfasst und zusammen verwendet, um unsere Fähigkeit zu verbessern, die Sprechereingaben aller Benutzer zu erkennen.

Wenn Sie Cortana die Berechtigung erteilen, erfassen wir ebenfalls Ihren Namen und Spitznamen, Ihre letzten Kalenderereignisse und die Namen der Personen mit denen Sie einen Termin haben, sowie Informationen über Ihre Kontakte einschließlich der Namen, Spitznamen, die Namen Ihrer Lieblingsorte, von Ihnen verwendete Apps, sowie Informationen über Ihre Musikeinstellungen. Diese zusätzlichen Daten erlauben es uns, Menschen, Ereignisse, Orte und Musik besser zu erkennen, wenn Sie Befehle, Nachrichten oder Dokumente diktieren.

Sie können die Cloud-Spracherkennung jederzeit deaktivieren. Dadurch wird die Datensammlung für diese Funktion beendet und die auf Ihrem Gerät gespeicherten zugehörigen Daten wie z. B. Ihr lokales Benutzerwörterbuch und Ihr Eingabeverlauf werden gelöscht.

Synchronisierungseinstellungen

Sobald Sie sich mit einem Microsoft-Konto bei Windows anmelden, synchronisiert Windows einige Ihrer Einstellungen und Daten mit den Microsoft-Servern, um die personalisierte Erfahrungen über mehrere Geräte hinweg einfacher zu gestalten. Nachdem Sie sich bei einem oder mehreren Geräten mit einem Microsoft-Konto angemeldet haben, lädt Windows beim ersten Anmelden an einem weiteren Gerät mit demselben Microsoft-Konto die Einstellungen und Daten herunter und übernimmt diese, die Sie für eine Synchronisierung Ihrer weiteren Geräte ausgewählt haben. Die von Ihnen für die Synchronisierung gewählten Einstellungen werden automatisch auf Microsoft-Servern und den weiteren Geräten aktualisiert, sobald diese von Ihnen verwendet werden.

Einige der Einstellungen, die synchronisiert werden, beinhalten:

- Apps, die Sie aus dem Microsoft Store installiert haben
- Spracheinstellungen
- Einstellungen für erleichterte Bedienung
- Personalisierungseinstellungen wie Kontobild, Hintergrund und Mauseinstellungen
- Einstellungen für Microsoft Store-Apps

- Wörterbücher für die Rechtschreibprüfung, Wörterbücher für den Eingabemethoden-Editor (IME) sowie persönliche Wörterbücher
- Browserverlauf, Favoriten und geöffnete Webseiten in Internet Explorer
- Gespeicherte Namen und Kennwörter von Apps, Webseiten, mobilen Hotspots und WLAN-Netzwerken

Über die Synchronisierungseinstellungen im Abschnitt „Konten“ der Windows-Einstellungen können festlegen, ob Sie Ihre Einstellungen synchronisieren möchten, und kontrollieren, was synchronisiert werden soll. Einige Apps verfügen über eigene separate Steuerelemente für die Synchronisierung. Wenn Sie sich bei Windows mittels eines Arbeitskontos anmelden und Sie dieses Konto auswählen um es mit Ihrem persönlichen Microsoft-Konto zu verbinden, dann wird Windows Sie danach fragen, welche Einstellungen Sie synchronisieren möchten, bevor Sie mit Ihrem Microsoft-Konto verbunden werden.

Aktualisierungsdienst

Der Aktualisierungsdienst für Windows enthält eine Windows-Aktualisierung und eine Microsoft-Aktualisierung. Die Windows-Aktualisierung ist ein Dienst, der Sie mit Software-Aktualisierungen für die Windows-Software und andere unterstützende Software wie z. B. gelieferte Treiber und Firmware vom Gerätehersteller versorgt. Microsoft Update ist ein Dienst, der Sie mit Softwareupdates für andere Microsoft-Software wie beispielsweise [Office](#) versorgt.

Windows Update lädt Windows-Software-Aktualisierungen automatisch auf Ihr Gerät herunter. Sie können Windows-Aktualisierungen so konfigurieren, dass diese Aktualisierungen automatisch installiert werden, sobald diese verfügbar sind (empfohlen) oder Sie durch Windows benachrichtigt werden, wenn ein Neustart erforderlich ist, um die Installation der Aktualisierungen abzuschließen. Apps, die im Microsoft Store verfügbar sind, werden automatisch über den Microsoft Store aktualisiert, wie im Abschnitt [Microsoft Store](#) weiter unten beschrieben wird.

Webbrowser: Microsoft Edge und Internet Explorer

Microsoft Edge ist der Standard-Webbrowser von Microsoft für Windows. Internet Explorer, der Vorgängerbrowser von Microsoft, steht in Windows ebenfalls zur Verfügung. Immer wenn Sie einen Webbrowser verwenden, um auf das Internet zuzugreifen, werden Daten über Ihr Gerät („Standardgerätedaten“) an die von Ihnen besuchten Webseiten und Onlinedienste gesendet. Standardgerätedaten umfassen die IP-Adresse Ihres Geräts, den Typ Ihres Browsers sowie die festgelegte Sprache, die Zugriffszeit und die aufgerufenen Webseitenadressen. Diese Daten werden möglicherweise auf den Web-Servern dieser Webseiten protokolliert. Welche Daten erfasst und wie diese Daten verwendet werden, hängt von den Datenschutzbestimmungen der von Ihnen besuchten Webseiten und Web-Diensten ab, die Sie verwenden.

Zusätzlich werden auf Ihrem Gerät Daten zur Nutzung Ihres Browsers gespeichert, z. B. Browserverlauf, Webformulardaten, temporäre Internetdateien und [Cookies](#). Sie können diese Daten von Ihrem Gerät mithilfe der Funktion Browserverlauf Löschen entfernen.

Neue Funktionen in Microsoft Edge erlauben Ihnen das Erfassen und Speichern von Inhalten auf Ihrem Gerät, wie zum Beispiel:

- **Webseitennotiz:** erlaubt Ihnen, Freihand- und Textanmerkungen auf den von Ihnen besuchten Webseiten und diese auszuschneiden, zu speichern oder zu teilen;
- **Active Reading:** erlaubt Ihnen, Leselisten, einschließlich Webseiten oder Dokumenten zu erstellen und zu verwalten; und
- **Hub:** erlaubt Ihnen, Ihre Leselisten, Favoriten, Downloads und den Verlauf in einem einzigen Bereich einfach zu verwalten.

Einige der Microsoft-Browser Informationen, die auf Ihrem Gerät gespeichert sind, werden über andere Geräte synchronisiert, sobald Sie sich mit Ihrem Microsoft-Konto anmelden. Zu diesen Informationen gehören in Internet Explorer z. B. Browserverlauf und Favoriten und in Microsoft Edge Favoriten und Leselisten. Wenn Sie in Microsoft Edge beispielsweise Ihre Leseliste auf verschiedenen Geräten synchronisieren, werden Kopien der Inhalte, die Sie für eine Speicherung in Ihre Leseliste auswählen, an jedes synchronisierte Gerät gesendet, um sie später betrachten zu können. Sie können die Synchronisierung in Internet Explorer deaktivieren, indem Sie die Synchronisierungseinstellungen im Abschnitt „Konten“ der Windows-Einstellungen aufrufen (siehe [Synchronisierungseinstellungen](#)). Sie können die Synchronisierung von Microsoft Edge Browser-Informationen auch deaktivieren, indem Sie die Synchronisierungsoption in den Microsoft Edge-Einstellungen deaktivieren.

Sowohl Microsoft Edge als auch Internet Explorer verwenden Ihre Suchanfragen und Ihren Browser-Verlauf, um Ihnen einen schnelleren Seitenaufbau und mehr relevante Treffer zu liefern. Diese Features umfassen:

- **Suchvorschläge** im Internet Explorer: Die Informationen, die Sie in die Adresszeile des Browsers eingeben, werden automatisch an Ihren Standardsuchanbieter (z. B. Bing) gesendet, der nach jedem eingegebenen Zeichen Suchvorschläge anzeigt.
- **Such- und Seitenvorschläge** in Microsoft Edge: Die Informationen, die Sie in die Adresszeile des Browsers eingeben, werden automatisch an Bing gesendet (auch wenn Sie einen anderen Standardsuchanbieter gewählt haben), damit nach jedem eingegebenen Zeichen Suchvorschläge angezeigt werden können.

Sie können diese Features jederzeit deaktivieren. Um Suchergebnisse zu liefern, senden sowohl Microsoft Edge als auch Internet Explorer Ihre Suchanfragen, Standard-Geräteinformationen, und den Standort (wenn Sie Standort aktiviert

haben) an Ihren Standardsuchanbieter. Wenn Bing Ihr Standardsuchanbieter ist, nutzen wir diese Daten wie im Abschnitt „Bing“ dieser Datenschutzbestimmungen beschrieben.

Cortana kann Sie bei Ihrem Webbrowsen in Microsoft Edge mit Funktionen wie „Cortana fragen“ unterstützen. Sie können die Unterstützung von Cortana für Microsoft Edge in den Microsoft Edge-Einstellungen jederzeit deaktivieren. Um mehr darüber zu erfahren, wie Cortana Daten nutzt und wie Sie dies steuern können, lesen Sie den Abschnitt [Cortana](#) in dieser Datenschutzerklärung.

WLAN-Netzwerkverbindung mit vorgeschlagenen öffentlichen Hotspots

Wenn Sie die Option „Mit vorgeschlagenen öffentlichen Hotspots verbinden“ in den WLAN-Einstellungen aktivieren, werden Sie automatisch mit vorgeschlagenen öffentlichen WLAN-Netzwerken verbunden. Bitte beachten Sie, dass nicht alle Netzzugänge sicher sind – seien Sie vorsichtig, wenn Sie mithilfe eines offenen Netzzugangs etwas online ausführen, das sensible oder persönliche Daten erfordert, beispielsweise eine Banktransaktion oder einen Kauf.

Windows Apps

Eine Reihe von Microsoft-Apps sind in Windows enthalten und weitere sind im Microsoft Store erhältlich. Einige dieser Apps enthalten:

Karten-App. Die Karten-App bietet positionsbezogene Dienste an und verwendet die Bing-Dienste, um Ihre Recherchen in der Karten-App zu verarbeiten. Beachten Sie den Abschnitt [Bing](#) in diesen Datenschutzbestimmungen, um weitere Informationen zu diesen von Bing bereitgestellten Features zu erhalten. Wenn die Maps-App Zugriff auf Ihren Standort hat, kann Microsoft anonymisierte Gerätepositionsdaten erfassen, die zur Verbesserung der Microsoft-Dienste beitragen, selbst wenn die App nicht verwendet wird. Sie können den Maps-App-Zugriff auf Ihren Standort deaktivieren, indem Sie den Positionsdienst oder den Maps-App-Zugriff auf den Positionsdienst deaktivieren.

Mit der Maps-App behalten Sie den Überblick über Ihre Lieblingsorte und die letzten Kartensuche. Ihre Lieblingsorte und Ihr Suchverlauf werden als Suchvorschläge aufgenommen werden. Wenn Sie mit Ihrem Microsoft-Konto angemeldet sind, werden Ihre Lieblingsorte, der Suchverlauf und bestimmte App-Einstellungen mit anderen Geräten und Diensten (z. B. Cortana) synchronisiert. Unter [Sync-Einstellungen](#) weiter oben finden Sie weitere Informationen.

Kamera- und Foto-Apps. Falls Sie der Kamera-App erlauben, Ihre Position zu verwenden, dann werden die Positionsdaten in den mit Ihrem Gerät aufgenommenen Fotos eingebettet. Weitere beschreibende Daten wie z. B. Kameramodell und das Datum, an dem das Bild aufgenommen wurde, sind ebenfalls in den Fotos und Videos eingebettet. Wenn Sie ein Foto oder Video teilen, werden alle eingebetteten Daten für die Personen und Dienste, mit denen

Sie diese teilen, zugänglich. Sie können den Kamera-App-Zugriff auf Ihren Standort deaktivieren, indem Sie den gesamten Zugriff auf den Positionsdienst im Einstellungsmenü Ihres Geräts oder den Kamera-App-Zugriff auf den Positionsdienst deaktivieren.

Ihre Fotos, Videos sowie Screenshots, welche in der Kamerarolle gespeichert sind, werden automatisch auf Microsoft OneDrive hochgeladen. Sie können sowohl Ihre Fotos und/oder Videos mittels Microsoft OneDrive verwalten als auch die automatische Aktualisierung in den Einstellungen deaktivieren.

Wenn Sie Fotos aufnehmen, in denen Ihr Standort eingebettet ist, dann kann die Foto-App Ihre Fotos nach Zeit und Standort gruppieren. Um Ihre Fotos zu gruppieren, sendet die Foto-App die Positionsdaten Ihrer Fotos an Microsoft, um die Namen von Standorten wie zum Beispiel „Seattle, Washington“ zu bestimmen. Wenn Sie die Foto-App verwenden, während Sie bei Ihrem Microsoft-Konto angemeldet sind, werden Ihre Fotos und Videos von Microsoft OneDrive automatisch in Alben in der Foto-App sortiert. Außerdem werden diese auf der Live-Kachel der Foto-App angezeigt. Ihre Fotos und/oder Videos werden nur dann mit anderen geteilt, wenn Sie uns dafür Ihre Zustimmung geben.

Kontakte-App. Mit der Kontakte-App können Sie mit all Ihren Kontakten zentral interagieren. Wenn Sie Ihr Microsoft-Konto zu einem Windows-Gerät hinzufügen, werden Ihre Kontakte automatisch von Ihrem Konto zur Personen-App hinzugefügt. Sie können weitere Konten der Personen-App hinzufügen, einschließlich denen von Ihren sozialen Netzwerken (z. B. Facebook und Twitter) und E-Mail-Konten. Wenn Sie ein Konto hinzufügen, werden Sie darüber informiert, welche Daten die Kontakte-App importieren oder mit dem entsprechenden Dienst synchronisieren kann. Anschließend können Sie die hinzuzufügenden Elemente auswählen. Andere Apps, die Sie installieren, können u. U. ebenfalls Daten mit der Kontakte-App synchronisieren, darunter zusätzliche Details zu bestehenden Kontakten. Sie können jederzeit ein Konto von der Kontakte-App entfernen.

App „Mail und Kalender“ Mit der App „Mail und Kalender“ können Sie alle E-Mails, Kalender und Dateien an einem Ort verknüpfen, einschließlich der von Drittanbieter-E-Mail- und Dateispeicheranbietern. Die App bietet positionsbezogene Dienste, wie z. B. Wetterinformationen in Ihrem Kalender, an. Sie können allerdings die Verwendung Ihrer Standortinformationen durch die App deaktivieren. Wenn Sie der App „Mail und Kalender“ ein Konto hinzufügen, werden E-Mail, Kalenderinformationen, Dateien, Kontakte und weitere Einstellungen von Ihrem Konto automatisch mit Ihrem Gerät und den Microsoft-Servern synchronisiert. Sie können jederzeit ein Konto entfernen oder die Daten ändern, die von Ihrem Konto synchronisiert werden. Um ein Konto zu konfigurieren, müssen Sie die Konto-Zugangsinformationen (wie Ihr Benutzername und Kennwort) in die App eingeben, die über das Internet an Drittanbieter-Server gesendet werden. Die App wird zunächst versuchen, eine sichere Verbindung (SSL) zu verwenden, um Ihr Konto zu konfigurieren, wird jedoch diese Informationen unverschlüsselt senden, wenn Ihr E-Mail-Anbieter SSL nicht unterstützt. Wenn Sie ein Unternehmenskonto

(z. B. die E-Mail-Adresse des Geschäfts/Unternehmens) hinzufügen, kann der Besitzer der Organisationsdomäne gewisse Richtlinien und Regelungen implementieren (z. B. eine mehrstufige Authentifizierung oder die Möglichkeit, Daten aus der Ferne zu löschen), die sich auf die Nutzung der App auswirken können.

Nachrichten-App. Wenn Sie sich mit einem Microsoft-Konto bei Ihrem Gerät anmelden können Sie auswählen, ob Sie eine Sicherungskopie Ihrer Information erstellen wollen, was dazu führt, dass Ihre SMS und MMS-Nachrichten synchronisiert und anschließend in Ihrem Microsoft-Konto gespeichert werden. Dadurch sind Sie in der Lage, Nachrichten abzurufen, wenn Sie Ihr Telefon verloren oder ersetzt haben. Nach Ihrer ersten Geräteeinrichtung sind Sie in der Lage, Ihre Nachrichteneinstellungen jederzeit zu verwalten. Das Ausschalten der SMS/MMS-Datensicherung führt nicht dazu, dass Nachrichten gelöscht werden, die zuvor auf Ihrem Microsoft-Konto gesichert wurden. Um solche Nachrichten aus dem Speicher zu löschen, müssen Sie diese von Ihrem Gerät löschen, bevor Sie die Datensicherung deaktivieren. Wenn Sie zulassen, dass die Nachrichten-App Ihren Standort verwendet, können Sie einen Link zu Ihrem aktuellen Standort an eine ausgehende Nachricht anhängen. Standortinformationen werden durch Microsoft, wie im [Positionsdienste](#) Abschnitt Windows-Ortungsdienst beschrieben, erhoben.

Die App „Brieftasche“ für Windows Phone. Mit der Brieftasche können Sie Informationen wie Coupons, Kundenkarten, Tickets und andere digitale Inhalte speichern. Sofern verfügbar, können Sie der Brieftasche auch Kreditkarten hinzufügen und mit diesen in teilnehmenden, NFC-fähigen Geschäften(near-Field Communication) zahlen.

Sie können die Brieftasche zur Zahlung einrichten, indem Sie sich mit Ihrem persönlichen Microsoft-Konto bei der Brieftasche anmelden und mit Ihrem Microsoft-Konto verknüpfte Kreditkarten hinzufügen. Wenn Sie der Brieftasche eine Kreditkarte hinzufügen, stellen wir Ihrer Bank und dem Kreditkarten-Netzwerk Daten zur Verfügung, wie Ihr Name, die Kreditkartennummer, die Rechnungsadresse, E-Mail-Adresse, Gerätedaten (einschließlich dem Namen, Typ und der Kennung Ihres Gerätes), sowie den Standort zu dem Zeitpunkt, an dem Sie der Brieftasche Ihre Kreditkarte hinzufügen. Diese Daten werden an Ihre Bank und an Ihr Karten-Netzwerk übermittelt, um die Berechtigung Ihrer Kreditkarte zu ermitteln, Transaktionen zu aktivieren und Betrugsversuche zu erkennen.

Wenn Sie eine NFC-Zahlung tätigen, stellt die Microsoft Brieftasche dem Händler eine verschlüsselte Version der Kreditkarte bereit (ein sog. „Token“). Der Händler übermittelt Ihrer Bank dieses Token zusammen mit den Details der Transaktion, um diese abzuschließen und eine Zahlung dafür anzufordern.

Windows Media Player

Mit Windows Media Player können Sie CDs, DVDs und andere digitale Inhalte abspielen (z. B. WMA- und MP3-Dateien), CDs kopieren und Ihre Medienbibliothek

verwalten. Um Ihre Erfahrungen beim Abspielen von Inhalten zu bereichern, zeigt Windows Media Player entsprechende Medieninformationen, wie z.B. den Titel des Albums, Titel des Stücks, Albumcover, Künstler oder Komponist und andere Informationen an. Um die Medieninformationen zu bereichern, sendet Windows Media Player eine Anfrage an Microsoft, die Standardcomputerinformationen enthält, eine ID für die Medieninhalte und bereits in der Windows Media Player-Bibliothek enthaltene Medieninformationen (einschließlich von Ihnen bearbeitete und eingegebene Informationen), damit Microsoft den Titel erkennt und zusätzliche verfügbare Informationen darüber zurück gibt.

Windows Media Player gibt ebenfalls Inhalte wieder, die über ein Netzwerk gestreamt werden. Um diesen Dienst bereitzustellen, muss Windows Media Player mit einem streamenden Medienserver kommunizieren. Diese Server werden in der Regel von einem anderen Inhaltsanbieter als Microsoft betrieben. Während der Medienstreamingwiedergabe sendet Windows Media Player ein Protokoll an den Medienserver oder an andere Webserver, wenn der streamende Medienserver dies anfordert. Das Protokoll enthält folgende Informationen: Verbindungszeit, IP-Adresse, Betriebssystemversion, Windows Media Player-Version, Player-ID (Player-ID), Datum und Protokoll. Um Ihre Privatsphäre zu schützen, sendet Windows Media Player standardmäßig eine Player-ID, die für jede Sitzung unterschiedlich ist.

Windows Hello

Windows-Hallo bietet über die biometrische Authentifizierung einen sofortigen Zugriff auf Ihre Geräte. Wenn Sie die Funktion aktivieren, verwendet Windows Hello Ihr Gesicht, Ihren Fingerabdruck oder Ihre Iris, um Sie anhand einer Reihe von eindeutigen Punkten oder Merkmalen, die aus dem Bild extrahiert werden und auf Ihrem Gerät als Vorlage gespeichert sind, zu identifizieren – das eigentliche Bild Ihres Gesichts oder Ihrer Iris wird jedoch nicht gespeichert. Biometrische Verifikationsdaten, die bei der Anmeldung verwendet werden, verlassen Ihr Gerät nicht. Sie können Ihre biometrischen Verifikationsdaten aus den Einstellungen löschen.

Windows Search

Mit der Windows Search können Sie eigene Informationen sowie das Web von einem Standort aus durchsuchen. Wenn Sie die Windows Search zur persönlichen Suche verwenden, werden Ergebnisse für Elemente zurückgegeben, die sich auf Ihrem persönlichen OneDrive, Ihrem OneDrive for Business (wenn aktiviert), auf anderen Cloud-Speicheranbietern (sofern diese Anbieter von Drittanbietern unterstützt werden) und auf Ihrem Gerät befinden. Wenn Sie Windows Search dazu nutzen, das Web zu durchsuchen oder Suchvorschläge über Windows Search oder Cortana zu erhalten, werden die Suchergebnisse von Bing bereitgestellt. Ihre Suchabfrage wird wie im Abschnitt [Bing](#) in diesen Datenschutzbestimmungen beschrieben behandelt.

Unterhaltung und ähnliche Dienste

Unterhaltung und ähnliche Dienste bieten eine komplexe Erfahrung und ermöglichen es Ihnen, auf eine Vielzahl von Inhalten, Anwendungen und Spielen zuzugreifen.

Xbox

Xbox-Konsolen sind Hardware-Geräte, die Sie für den Zugriff und das Spielen von Spielen, Filmen, Musik und andere Formen der digitalen Unterhaltung verwenden können. Xbox Live (einschließlich der Spiele für Windows Live) ist der Entertainment-Dienst und das soziale Netzwerk für Online-Spiele von Microsoft. Es bietet Ihnen die Möglichkeit, sich mit Ihren Freunden auf Xbox Live und anderen Spiel- und sozialen Netzwerken zu verbinden. Xbox-Dienste können auf einer Vielzahl von Geräten verwendet werden, einschließlich Xbox-Konsolen, PCs (auch über xbox.com und die Xbox-App) und mobilen Geräten.

Wir erheben Daten über Ihre Benutzung der Xbox-Dienste wie zum Beispiel:

- Sobald Sie sich an- und abmelden, die von Ihnen gespielten Spiele, Ihre Spiel- und Ergebnisstatistiken und die Einkäufe, die Sie tätigen sowie die Inhalte, die Sie erhalten.
- Leistungsdaten über die Xbox-Dienste, das Gerät und die Netzwerkverbindung einschließlich auftretende Hardware- oder Software-Fehler.
- Falls Sie die Xbox-Konsole mit Kinect verwenden auch Daten darüber wie Sie Kinect verwenden. Nachfolgend finden Sie weitere Informationen über die Kinect-Datenerfassung.

All diese Daten werden mit der eindeutigen Kennung der Xbox-Konsole gespeichert und mit Ihren persönlichen Daten verbunden. Wenn Ihre Xbox mit dem Internet verbunden ist, können wir feststellen, welche Xbox-Konsole und welche Version des Xbox Dashboards Sie zurzeit verwenden.

Mit Ihrer Zustimmung werden wir Informationen über Videos erheben, die Sie über Drittanbieter-Anwendungen, auf Ihrer Xbox-Konsole gekauft oder betrachtet haben. Wenn Sie die Xbox TV App nutzen, erfassen wir den TV-Anzeigeverlauf von Ihrer Konsole in einer Weise, bei der weder Sie noch andere Personen identifiziert werden.

Wenn Sie eine Xbox-Konsole verwenden, die über ein Speichermedium verfügt (Festplatte oder Speichereinheit) und Sie offline spielen oder sich nie beim Dienst registriert haben, werden die Nutzungsdaten auf dem Speichermedium der Xbox-Konsole gespeichert und bei der nächsten Anmeldung dem befindlichen Dienst an Microsoft gesendet.

Xbox Live-Daten, die für andere Benutzer sichtbar sind. Ihre Gamertag- (Xbox Live-Spitzname), Spiel- und Score-Statistiken, Errungenschaften, Präsenz (ob Sie bei

Xbox Live angemeldet sind) und andere Daten über Ihre Aktivitäten auf Xbox Live oder andere Eigenschaften im Zusammenhang mit Xbox Live (auch die der Partnerunternehmen) können von anderen Benutzern auf Xbox Live betrachtet werden. Zum Beispiel werden Ihr Gamertag und Ergebnisse, die auf Spiel-Bestenlisten gezeigt werden als öffentlich angesehen und können nicht verborgen werden. Für andere Arten von Daten können Sie Ihre Datenschutzeinstellungen auf der Konsole anpassen oder auf xbox.com den Austausch mit anderen Nutzern über xbox.com begrenzen oder blockieren.

Xbox Live-Daten, die mit Spiel- oder App-Herausgebern geteilt werden. Wenn Sie ein für Xbox Live geeignetes Spiel oder App verwenden, dann hat der Herausgeber oder Dienstanbieter dieses Spiels oder der App Zugriff auf Daten hinsichtlich Ihrer Nutzung von Xbox Live oder des Spiels oder der App und wird diese Daten möglicherweise veröffentlichen oder anzeigen (wie z. B. in Bestenlisten). Zu diesen Daten gehören beispielsweise Ihre Spielergebnisse, Daten über Ihre Spielsitzungen (z. B. Fahrzeugtypen, die im Spiel verwendet werden), Ihre Präsenz auf Xbox Live, die Zeit, die Sie zum Spielen des Spiels oder der App aufwenden, Bestenlisten, Statistiken, Spielerprofile, Avatare und andere Inhalte, die Sie innerhalb des Spiels oder der App erstellen oder übermitteln.

Die Verknüpfung Ihres Xbox Live-Kontos mit Nicht-Microsoft-Konten. Einige der Spiele oder Apps, die Sie auf Xbox Live finden, werden von Partnerunternehmen bereitgestellt, die möglicherweise von Ihnen verlangen, ein Nicht-Microsoft-Konto und Anmeldeinformationen zu erstellen, um das Spiel oder die App zu verwenden. Wenn Sie Ihr Microsoft-Konto mit Ihrem Konto bei einem Partnerunternehmen verlinken, wird Microsoft begrenzte Kontoinformationen mit diesem Unternehmen austauschen. Solche Kontoinformationen können Name, Adresse, E-Mail und Geburtsdatum enthalten, jedoch keine Kreditkarten- oder andere Zahlungsinformationen. Für Spiele, die eine Im-Spiel-Kommunikation ermöglichen, wird der Spieleherausgeber auch Zugriff auf den Inhalt der Im-Spiel-Kommunikation bekommen, sobald Sie sich bei Ihrem Konto dieses Herausgebers anmelden.

Kinect. Der Kinect Sensor ist eine Kombination aus Kamera, Mikrofon und Infrarot-Sensor, der Bewegungen und Stimmen aktivieren kann, um den Spielverlauf zu steuern und innerhalb des Dienstes zu navigieren. Zum Beispiel:

- Einmal ausgewählt, kann die Kamera dafür verwendet werden, um Sie automatisch mittels Gesichtserkennung am Dienst anzumelden. Es tut dies, indem es ein Bild des Gesichts aufnimmt und die Abstände zwischen den Schlüsselpunkten misst, um einen numerischen Wert zu erstellen und zu speichern, der nur Sie repräsentiert. Diese Daten verbleiben auf der Konsole und werden nicht an Dritte weitergegeben, und Sie können sich jederzeit dazu entscheiden, diese Daten von der Konsole zu löschen.
- Für den Spielverlauf misst Kinect die Abstände zwischen den Gelenken Ihres Körpers, um damit eine Art Strichmännchen von Ihnen zu erstellen und so den Spielverlauf zu ermöglichen. Sobald Sie online spielen, erheben wir

solche numerischen Werte, die den Spielverlauf und das Spielerlebnis aktivieren und verbessern. Kinect erkennt auch bestimmte Handgesten, die einfache System-Interaktionen (wie Menü-Navigation, Pan / Zoom und Scroll) bewirken sollen.

- Für einige der Fitness-Spiele kann die Xbox den Kinect-Sensor dafür verwenden, Ihre Trainingsdaten zu bestimmen, einschließlich Schätzungen Ihrer Herzfrequenz während einer bestimmten Aktivität oder die Anzahl der Kalorien, die während des Trainings verbraucht werden.
- Die Kinect-Mikrofone ermöglichen während des Spiels einen Voice-Chat zwischen Spielern. Sie ermöglichen auch Sprachbefehle zur Steuerung von Konsole, Spiel oder App oder für die Eingabe von Suchbegriffen. Nachfolgend finden Sie weitere Informationen über die Voice-Datenerfassung.
- Der Kinect Sensor kann auch für die Audio- und Videokommunikation über Dienste wie [Skype](#) verwendet werden.

Mehr über Kinect für Xbox 360 erfahren Sie unter [Datenschutz bei Kinect und Xbox 360](#). Für Xbox One finden Sie weitere Informationen unter [Datenschutz bei Kinect und Xbox One](#).

Untertitel. Beim Echtzeit-Chat mit Xbox können Spieler ein Feature zu aktivieren, das es ermöglicht, die im Spiel gesprochene Chat-Kommunikation als Text anzuzeigen. Wenn ein Benutzer dieses Feature aktiviert, werden die anderen Spieler nicht darüber unterrichtet. Microsoft verwendet diese Daten, um Untertitel für Benutzer hinzuzufügen, die diese Texte benötigen. Wir verwenden diese Daten auch zur Verbesserung dieses Diensts und ähnlicher sprachbezogener Dienste.

Kommunikationsüberwachung. Xbox Live enthält Kommunikationsfeatures, wie beispielsweise textbasierte Nachrichten und Onlinesprachchats zwischen Spielern während des Spiels. Damit wir eine sichere Spielumgebung bereitstellen und die [Verhaltensregeln von Microsoft](#) durchsetzen zu können, erfassen, überprüfen und überwachen wir stichprobenartig die Kommunikationen, einschließlich der Xbox Live-Spiel-Chats und Gruppen-Chats in live gehosteten Multiplayer-Spielverlaufssitzungen, die durch diese Dienste angeboten werden.

Sprachdaten für die Verbesserung des Dienstes. Für die Verbesserung des Dienstes erheben und verwenden wir Sprachsuchanfragen oder Proben von Sprachbefehlen, die während der Nutzung von Kinect verwendet werden. Diese Daten werden getrennt von Ihrem Xbox-Profil gespeichert.

GameDVR. Jeder Spieler in einer Multiplayer-Spielsitzung kann GameDVR verwenden, um seine Sicht des Spielverlaufs in dieser Sitzung aufzuzeichnen. Die Aufnahme kann Ihren Charakter innerhalb des Spiels und Ihren Gamertag in den Spiel-Clips erfassen, die von anderen Spielern in der Spielsitzung erstellt wurden. Beachten Sie, dass, falls ein Spieler GameDVR auf einem PC verwendet, Audio-Chat ebenfalls in einem Spiel-Clip festgehalten werden kann. Microsoft kann Spielclips auf Verstöße gegen die [Verhaltensregeln von Microsoft](#) überprüfen, auch wenn die Freigabeeinstellung für Spielclips blockiert wurde.

Xbox Live Rewards. Xbox Live Rewards, erhältlich unter rewards.xbox.com, ist ein Programm, dem Sie beitreten können, um Xbox-Guthaben dafür zu erhalten, dass Sie die Dienste aktiv verwenden. Sie müssen sich dazu verpflichten, Werbemitteilungen vom Prämien-Programm als Bedingung für eine Mitgliedschaft erhalten zu wollen. Sie können sich mit Ihrem Microsoft-Konto bei Rewards anmelden, das Programm erhebt dann persönliche Daten, einschließlich Vorname, Nachname, Gamertag und demographische Informationen. Das Programm wird von HelloWorld, einem Microsoft-Anbieter, gehostet und betrieben. Die erhobenen Daten werden durch den Anbieter im Auftrag von Microsoft gespeichert. Die persönlichen Daten, die Sie im Rahmen des Rewards-Programms angeben, können Sie über den Kontakt zu privacy@helloworld.com einsehen und bearbeiten.

Kinder- und Onlineschutz. Wenn Sie Kinder haben, die den Xbox-Dienst verwenden möchten, können Sie Kinderkonten für sie einrichten. Kinder unter 17 Jahren dürfen ohne Genehmigung der Erziehungsberechtigten kein Konto für Xbox Live erstellen. Erwachsene innerhalb der Familie können die Zustimmungsauswahl und Online-Sicherheitseinstellungen für Kinderkonten auf xbox.com ändern.

Microsoft Store

Der Microsoft Store ist ein Onlinedienst, mit dem Sie Anwendungen und andere digitale Inhalte durchsuchen, herunterladen, kaufen, bewerten und überprüfen können. Es enthält Folgendes:

- Apps und Inhalte für Windows-Geräte, wie z. B. Mobiltelefone, PCs und Tablets,
- Spiele und andere Apps für Xbox-Konsolen und
- Produkte und Apps für Office, SharePoint, Exchange, Access und Project (alle ab Version 2013).

Wir erfassen Daten zu Ihrem Zugriff auf den Microsoft Store und die von Ihnen angezeigten, gekauften oder installierten Produkte, zu den Präferenzen, die Sie für das Anzeigen von Apps im Microsoft Store festgelegt haben, sowie über alle Bewertungen, Beurteilungen und Problemlberichte, die Sie übermitteln. Ihr Microsoft-Konto ist mit Ihren Bewertungen und Beurteilungen verbunden, und sobald Sie eine Beurteilung verfassen wird der Name und das Bild von Ihrem Microsoft-Konto gemeinsam mit Ihrer Beurteilung veröffentlicht.

Berechtigung für Microsoft Store-Apps. Viele Apps, die Sie aus dem Microsoft Store installieren, sind so konzipiert, dass sie bestimmte Hardware- und Software-Features Ihres Gerätes verwenden. Die Verwendung bestimmter Hardware- und Softwarefunktionen durch eine App kann sowohl der App als auch dem damit verbundenen Dienst Zugriff auf Ihre Daten geben. Zum Beispiel könnte eine Fotobearbeitungs-App auf Ihr Gerät zugreifen, um Ihnen zu ermöglichen, ein neues Foto zu machen oder auf gespeicherte Fotos oder Videos auf Ihrem Gerät zum Zwecke der Bearbeitung zuzugreifen, und ein Restaurantführer könnte anhand Ihres Standorts Empfehlungen für die Umgebung anbieten. Informationen zu den

Funktionen, die von einer App verwendet werden, sind in der App-Produktbeschreibungsseite im Microsoft Store erhältlich. Viele der von den Microsoft Store-Apps verwendeten Features können in den Datenschutzeinstellungen Ihres Gerätes aktiviert und deaktiviert werden. Unter Windows können Sie in vielen Fällen auswählen, welche Apps eine bestimmte Funktion verwenden können. Wechseln Sie zur **Startseite > Einstellungen > Datenschutz**. Wählen Sie die Funktion aus (z. B. „Kalender“) und wählen Sie dann aus, welche App-Berechtigungen aktiviert oder deaktiviert werden sollen. Die Listen der Apps in den Windows-Datenschutzeinstellungen, die Hardware- und Software-Features verwenden können, enthalten nicht die klassischen Windows-Apps, und diese sind nicht von den Einstellungen betroffen.

App-Updates. Sofern Sie die automatischen App-Updates in den relevanten Microsoft Store-Einstellungen nicht deaktiviert haben, wird der Microsoft Store automatisch überprüfen, ob App-Updates heruntergeladen und installiert werden können, um sicherzustellen, dass Sie über die neuesten Versionen verfügen. Aktualisierte Apps können möglicherweise unterschiedliche Windows-Hardware- und Softwarefunktionen aus früheren Versionen verwenden, die ihnen einen Zugang zu unterschiedlichen Daten auf Ihrem Gerät geben können. Sie werden zur Zustimmung aufgefordert, sobald eine aktualisierte App auf bestimmte Funktionen wie zum Beispiel den Standort zugreifen möchte. Sie können auch die von einer App verwendeten Hardware- und Softwarefeatures überprüfen, indem Sie die Produktbeschreibungsseite im Microsoft Store anzeigen.

Jede Nutzung Ihrer Daten durch eine App, die durch eine dieser Funktionen gesammelt wurden, unterliegt den Datenschutzbestimmungen des jeweiligen App-Entwicklers. Wenn eine über den Microsoft Store erhältliche App Ihre persönlichen Daten sammelt und verwendet, wird vom App-Entwickler verlangt, eine Datenschutzerklärung zur Verfügung zu stellen, und ein Link zu den Datenschutzbestimmungen ist auf der App-Produktbeschreibungsseite im Microsoft Store verfügbar.

Sideload-Apps und Entwicklermodus. Entwickler-Features wie die „Entwicklermodus“-Einstellung sind nur für den Entwicklungsgebrauch bestimmt. Wenn Sie Entwickler-Funktionen aktivieren, kann Ihr Gerät unzuverlässig oder unbrauchbar werden, und Sie Sicherheitsrisiken aussetzen. Mit dem Herunterladen oder dem anderweitigen Erwerb von Apps außerhalb des Microsoft Store, auch „Sideloaden“ von Apps genannt, können Ihr Gerät und Ihre persönlichen Daten anfälliger für einen Angriff oder eine unvorhergesehene Verwendung durch Apps werden. Die Windows-Richtlinie, Benachrichtigungen, Zugriffsrechte und andere Funktionen, die dazu beitragen sollen, Ihre Privatsphäre zu schützen, sobald Apps auf Ihre Daten zugreifen, funktionieren bei Verwendung von Sideload-Apps oder im Falle dass Entwicklerfunktionen aktiviert sind möglicherweise nicht, wie in dieser Erklärung beschrieben.

MSN

MSN-Dienste enthalten Webseiten und eine Suite von Apps, einschließlich MSN Nachrichten, Wetter, Sport, Finanzen und frühere Versionen der Apps, die noch mit Bing (zusammen „MSN-Apps“) gekennzeichnet waren. Die MSN-Apps sind auf verschiedenen Plattformen wie Windows, iOS und Android verfügbar. MSN-Dienste sind auch in anderen Microsoft-Diensten enthalten, einschließlich dem Browser Microsoft Edge.

Sobald Sie MSN-Apps installiert haben, erheben wir Informationen, die uns mitteilen, ob die App ordnungsgemäß installiert wurde, das Installationsdatum, die App-Version und weitere Informationen über Ihr Gerät wie z. B. Betriebssystem und Browser. Diese Daten werden auf einer regelmäßigen Basis erhoben, die uns dabei hilft, die Anzahl der MSN-App-Benutzer zu bestimmen und Performance-Probleme im Zusammenhang mit verschiedenen App-Versionen, Betriebssystemen und Browsern zu identifizieren.

Wir erheben auch Daten darüber, wie Sie Ihre MSN-Dienste nutzen, zum Beispiel Nutzungshäufigkeit und angezeigte Inhalte, um Ihnen relevante Inhalte bereitzustellen. Einige MSN-Dienste bieten eine erweiterte Erfahrungsmöglichkeit an, sobald Sie sich mit Ihrem Microsoft-Konto anmelden, einschließlich der Möglichkeit, Ihre Interessen und Favoriten anzupassen. Sie können die Personalisierung über MSN- und Bing-Einstellungen sowie über Einstellungen in anderen Microsoft-Diensten, die MSN-Dienste enthalten, anpassen. Die Daten werden von uns auch dafür erhoben, um Sie mit Werbung zu versorgen, die für Sie von Interesse sein könnte. Über die Werbelinks innerhalb der MSN-Dienste oder auf der [Opt-Out-Seite](#) von Microsoft können Sie den Empfang interessenbezogener Werbung ablehnen.

Frühere Versionen von MSN Money ermöglichen es Ihnen, an persönliche Finanzinformationen von Drittanbieter-Finanzinstituten zu gelangen. MSN Money zeigt diese Informationen lediglich an, es speichert sie jedoch nicht. Ihre Anmeldeinformationen für den Zugang zu Ihren finanziellen Informationen von Drittanbietern sind auf Ihrem PC verschlüsselt und werden nicht an Microsoft gesandt. Diese Finanzinstitute sowie alle anderen Dienste von Drittanbietern auf welche Sie über MSN-Dienste zugreifen können, unterliegen deren eigenen Bedingungen und Datenschutzrichtlinien.

Groove-Musik/Filme & TV

Mit Groove Music können Sie auf einfache Weise Ihre Musiksammlung wiedergeben, Wiedergabelisten zusammenstellen, Musikstücke erwerben und angepasste Radiosender übertragen. Microsoft Movies & TV erlaubt Ihnen das Abspielen Ihrer Video-Sammlung sowie das Ausleihen oder Kaufen von Filmen und Folgen von Fernsehserien. Diese Dienste wurden früher als Xbox Music und Video angeboten.

Um sie beim Auffinden von Inhalten zu unterstützen, die Sie interessieren könnten, erhebt Microsoft Daten darüber, welche Inhalte Sie abspielen, die Länge des

Abspielens und die von Ihnen vergebene Beurteilung. Wenn Sie sich bei Cortana auf Ihrem Gerät anmelden, erhebt Microsoft Daten in Bezug auf die Musik, die Sie über Groove Music abspielen und verwendet diese, um personalisierte Erfahrungen und zutreffende Anregungen zu geben.

Um Ihre Erfahrungen beim Abspielen von Inhalten zu bereichern, zeigen Groove Music sowie Movies & TV entsprechende Informationen über die von Ihnen abgespielten Inhalte sowie die Inhalte in Ihren Musik- und Videosammlungen, wie z.B. den Titel des Albums, Bilder vom Album, Titel des Stücks oder Videos und andere Informationen an, falls diese verfügbar sind. Um diese Informationen zur Verfügung zu stellen, senden Groove Music und Movies & TV Informationen an Microsoft, die Standardgerätedaten enthalten, wie z.B. die IP-Adresse Ihres Gerätes, die Software-Version Ihres Gerätes, Ihre Region- und Spracheinstellungen und ein Identifikator für den Inhalt.

Wenn Sie Groove-Musik oder Filme & TV verwenden, um auf Inhalte zuzugreifen, die mit Microsoft Digital Rights Management (DRM) geschützt sind, werden automatisch Mediennutzungsrechte von einem Onlinerechteserver angefordert und DRM-Updates heruntergeladen und installiert, um die Inhalte abspielen zu können. In den DRM-Informationen im Abschnitt [Silverlight](#) in diesen Datenschutzbestimmungen finden Sie weitere Details.

Silverlight

Microsoft Silverlight hilft Ihnen, auf reichhaltige Inhalte im Web zuzugreifen und diese zu genießen. Silverlight ermöglicht es Webseiten und Diensten auf Ihrem Gerät zu speichern. Weitere Silverlight-Funktionen beinhalten das Einrichten einer Verbindung zu Microsoft, um Aktualisierungen zu erhalten oder zu Microsoft oder zu Servern von Drittanbietern, um geschützte digitale Inhalte wiederzugeben.

Das Konfigurationstool von Silverlight. Sie können eine Auswahl für diese Features im Silverlight-Konfigurationstool vornehmen. Um auf das Silverlight-Konfigurationstool zugreifen zu können, klicken Sie rechts auf Inhalte, die derzeit von Silverlight angezeigt werden und **Silverlight**. Sie können das Silverlight-Konfigurationstool auch direkt ausführen. In Windows können Sie beispielsweise auf das Tool zugreifen, indem Sie nach „Microsoft Silverlight“ suchen.

Silverlight-Appspeicher. Silverlight-basierte Apps können Datendateien lokal auf Ihrem Computer für eine Vielzahl von Zwecken abspeichern, einschließlich dem Speichern Ihrer benutzerdefinierten Einstellungen, dem Speichern von großen Dateien für grafikintensive Features (z. B. Spiele, Karten und Bilder) sowie dem Speichern von Inhalten, die Sie innerhalb bestimmter Anwendungen erstellen. Sie können den Appspeicher im Silverlight-Konfigurationstool deaktivieren oder konfigurieren.

Silverlight Updates. Silverlight wird in regelmäßigen Abständen einen Microsoft-Server auf Updates überprüfen, um Ihnen die neuesten Features und

Verbesserungen zur Verfügung zu stellen. Eine kleine Datei, die Informationen über die aktuelle Silverlight-Version enthält, wird auf Ihren Computer heruntergeladen und mit Ihrer aktuell installierten Version verglichen. Falls eine neuere Version verfügbar ist, wird diese heruntergeladen und auf Ihrem Computer installiert. Sie können im Silverlight-Konfigurationstool Updates konfigurieren oder deaktivieren.

Verwaltung digitaler Rechte. Silverlight verwendet Microsoft Digital Rights Management (DRM), um die Rechte der Eigentümer von Inhalten zu schützen. Wenn Sie auf DRM-geschützte Inhalte (wie Musik oder Video) mittels Silverlight zugreifen, wird es Mediennutzungsrechte von einem Rechteserver im Internet beantragen. Um ein nahtloses Wiedergabeerlebnis zu ermöglichen, erhalten Sie keine Aufforderung, bevor Silverlight die Anforderung an den Rechteserver sendet. Während des Anforderns von Mediennutzungsrechten wird Silverlight dem Rechteserver eine ID für die DRM-geschützte Inhaltsdatei sowie grundlegende Daten über Ihr Gerät zur Verfügung stellen, einschließlich der Daten über die DRM-Komponenten auf Ihrem Gerät wie Version und Sicherheitsstufen sowie einer eindeutigen Kennung für Ihr Gerät.

DRM-Updates. In einigen Fällen kann der Zugriff auf DRM-geschützte Inhalte ein Update für Silverlight oder für die DRM-Komponenten des Gerätes erforderlich machen. Wenn Sie versuchen Inhalte abzuspielen, die ein DRM-Update erfordern, wird Silverlight eine Anfrage an einen Microsoft-Server senden, die grundlegende Daten über Ihr Gerät, einschließlich Informationen über die DRM-Komponenten auf Ihrem Computer wie Version und Sicherheitsstufen, Fehlerdaten sowie eine eindeutige Kennung für Ihr Gerät enthält. Der Microsoft-Server verwendet diese Kennung, um eine eindeutige DRM-Aktualisierung für Ihr Gerät zurückzugeben, die dann von Silverlight installiert wird. Sie können das Konfigurieren der DRM-Komponenten-Aktualisierung auf der **Playback**-Registerkarte im Silverlight-Konfigurationstool deaktivieren.

Microsoft Health-Dienste

Microsoft Health-Dienste ermöglicht das Erfassen und Verwalten von Gesundheitsdaten. Dazu gehören HealthVault, HealthVault-Einblicke, Microsoft Band-Geräte und andere Microsoft Health-Apps und zugehörige Produkte. Das Band unterstützt Sie dabei, Daten, wie Herzschlag und vergangene Schritte, nachzuverfolgen. Das Band kann zudem Cortana verwenden, um Notizen zu machen und Benachrichtigungen von Ihrem Telefon zu erhalten. Die Microsoft Health-App sendet Daten an Microsoft-Server und ermöglicht Ihnen die Ansicht, Verwaltung und Kontrolle der Daten. Apps können Benachrichtigungen an das Band und andere Geräte senden. Mit HealthVault-Diensten können Sie Gesundheitsdaten sammeln, bearbeiten, hinzufügen und online speichern und diese mit Ihrer Familie, Ihren Betreuern und medizinischen Fachkräften austauschen.

Microsoft Health-Dienste erhebt und verwendet Ihre Daten für die Bereitstellung der Dienste, einschließlich der Verbesserung und Personalisierung Ihrer Erfahrung. Gesundheitsdaten, die Sie über Microsoft Health-Dienste in Microsoft bereitstellen, werden nicht mit den Daten anderer Microsoft-Dienste kombiniert und werden ohne Ihre

ausdrückliche Zustimmung nicht für andere Zwecke verwendet. Beispielsweise nutzt Microsoft Ihre Patientenakte nicht ohne Ihre Zustimmung, um Werbung an Sie zu senden.

Health-Dienste

Microsoft Health-Dienste ermöglicht das Erfassen und Verwalten von Gesundheitsdaten. Die erhobenen Daten hängen von den Diensten und Funktionen ab, die Sie verwenden und enthalten Folgendes:

- **Profildaten.** Wenn Sie ein Profil erstellen, müssen Sie Daten wie beispielsweise Größe, Gewicht und Alter angeben, die zur Berechnung der Aktivitätsergebnisse verwendet werden. Weitere Profildaten stammen aus Ihrem persönlichen [Microsoft-Konto](#).
- **Aktivitäts- und Fitnessdaten.** Mithilfe von Microsoft Health-Diensten können Sie Aktivitäts- und Fitnessdaten wie Ihre Herzfrequenz, Schritte, verbrannte Kalorien und Schlaf im Auge behalten. Beispiele für Arten an Aktivitäten, die Sie zur Nachverfolgung auswählen können, sind Jogging-Läufe, Trainingseinheiten und Schlaf.
- **Nutzungsdaten.** Um Ihnen den bestmöglichen Dienst bieten zu können, erfassen und laden wir automatisch Statistiken über die Leistung und Ihre Verwendung der Microsoft Health-Dienste hoch.
- **Position.** Microsoft Band besitzt integrierte GPS (Global Positioning System) -Features, mit denen Sie Aktivitäten wie Joggen oder Fahrradfahren abbilden können, ohne dass Sie Ihr Handy mitführen müssen. Wenn Sie GPS für eine Aktivität aktivieren, können Sie die Aktivitätskarte in der Microsoft Health-App betrachten. Einige Modi von Band, z. B. Golf und Explorer, schalten automatisch das GPS ein und es dann bei Beenden des Modus wieder aus.

Weitere Informationen zu den Sensoren von Microsoft Band und dem Sammeln von Daten finden Sie unter [hier](#).

Zugriff und Steuerung. Sie können Ihre Daten in Microsoft Health-Dienste anzeigen und verwalten. Sie können Ihre Profildaten einsehen und aktualisieren, verbundene Anwendungen verwalten und vergangene Aktivitäten betrachten. Sie können die Einzelheiten spezieller Aktivitäten in der Microsoft Health-Dienst löschen. Wenn Sie eine spezielle Aktivität löschen, wird das Ereignis aus dem Microsoft Health-Dienst gelöscht; aber die von den Geräten erfassten Basissensordaten und andere Daten verbleiben im Microsoft Health-Dienst. Sie können Ihren Microsoft Health-Dienst jederzeit kündigen. Wenden Sie sich dazu an den Kundendienst [Hier](#).

Cortana. Die Microsoft Health-Diensten ermöglichen das Verwenden von Cortana. Mit Cortana werden die in den Microsoft Health-Diensten verarbeiteten Daten, einschließlich gesundheitsbezogener Daten und Daten von Drittanbieterdiensten, für Cortana freigegeben. Mithilfe der Funktionen von Cortana können Sie Notizen machen, Abfragen durchführen und Erinnerungen per Sprache festlegen, wenn [Cortana](#) auf Ihrem Gerät aktiviert ist. Weitere Informationen darüber, wie [Cortana](#)

Ihre Daten verwaltet, finden Sie im Abschnitt „Cortana“ dieser Datenschutzbestimmungen.

HealthVault

HealthVault ist eine persönliche Gesundheitsplattform, die es Ihnen erlaubt, Gesundheitsdaten online zu erfassen, zu bearbeiten, zu speichern sowie ihre Gesundheitsdaten auszutauschen. Mit HealthVault können Sie Ihre eigenen Patientenakten überwachen. Sie können sich auch dafür entscheiden, Ihre Gesundheitsdaten mit Ihrer Familie, Ihrem Pflegepersonal, Ihren medizinischen Fachkräften, mobilen Apps, gesundheitsbezogenen Geräten und Onlinetools auszutauschen. Weitere Informationen über HealthVault finden Sie unter [hier](#).

Anmeldung bei HealthVault. Um sich bei HealthVault anzumelden, können Sie [Microsoft-Konto](#) oder Drittanbieter-Authentifizierungsdiensten verwenden. Wenn Sie Ihr Microsoft-Konto löschen oder Ihre Konto-Zugangsinformationen verlieren, sind Sie möglicherweise nicht mehr in der Lage, auf Ihre Daten zuzugreifen. Sie können mehr als eine Art von Zugangsinformationen mit HealthVault verwenden, um einen fortlaufenden Zugang sicherzustellen. Bevor Sie Drittanbieter-Authentifizierungsdienste mit HealthVault verwenden empfehlen wir Ihnen, die von diesem Herausgeber angebotenen Sicherheits- und Datenschutzverpflichtungen zu überprüfen.

HealthVault-Konto und Health-Patientenakten. Um ein neues HealthVault-Konto anzulegen, müssen Sie persönliche Daten, wie beispielsweise Ihren Namen, das Geburtsdatum, die E-Mail-Adresse, die PLZ und das Land/die Region angeben. Abhängig von den Funktionen, die Sie verwenden, werden Sie möglicherweise nach zusätzlichen Informationen gefragt. Ein HealthVault-Konto erlaubt Ihnen die Verwaltung von einer oder mehreren Patientenakten, beispielsweise diejenigen, die Sie für sich selbst oder für Ihre Familienangehörigen anlegen. Sie können Daten zu einer Patientenakte, die Sie verwalten, jederzeit hinzufügen oder löschen.

HealthVault weist in den USA jeder Patientenakte eine einzigartige Health Vault-E-Mail-Adresse zu. Wenn eine Nachricht unter dieser E-Mail-Adresse eingeht, wird die Nachricht und die Anhänge automatisch zur HealthVault-Patientenakte hinzugefügt, und es erfolgt eine E-Mail-Benachrichtung an die Treuhänder dieser Patientenakte. Der E-Mail-Dienst in HealthVault verwendet „Direct“, ein Protokoll, das speziell für die Kommunikation mit Gesundheitsdienstleistern ausgelegt ist. Aus diesem Grund kann eine HealthVault-E-Mail nur von Diensteanbietern gesendet und empfangen werden, die ein für Direct-Protokoll eingerichtetes System verwenden. Treuhänder können E-Mail-Adressen von Patientenakten hinzufügen oder deaktivieren.

Freigabe von Health-Daten. Ein entscheidender Vorteil von HealthVault ist die Möglichkeit, dass Sie Ihre Gesundheitsdaten mit Personen und Diensten teilen können, die Ihnen bei der Erreichung Ihrer Gesundheitsziele behilflich sein können. Standardmäßig sind Sie der Treuhänder derjenigen Akten, die Sie anlegen.

Treuhänder haben die höchste Zugriffsebene zu einer Patientenakte. Als Treuhänder können Sie Daten aus einer Patientenakte mit einer anderen Person austauschen, indem sie eine E-Mail-Einladung über HealthVault senden. Sie können angeben, welchen Zugriff diese haben sollen (einschließlich dem Treuhänder-Zugriff), wie lange sie Zugriff haben sollen und ob sie die Daten in der Akte modifizieren können. Wenn Sie jemandem Zugriff gewähren, kann diese Person dieselbe Zugriffsebene an einen Dritten gewähren (zum Beispiel kann jemand mit einem Zugriff nur zum Anzeigen einem Dritten einen entsprechenden Zugriff nur zum Anzeigen gewähren). **Da eine ungeeignete Gewährung eines Zugriffs es jemandem ermöglichen könnte, Ihre Privatsphäre zu verletzen oder sogar den Zugriff auf Ihre eigene Patientenakte zu unterbinden, müssen Sie bei der Gewährung eines Zugriffs auf Ihre Patientenakte vorsichtig sein.**

Sie können auswählen, spezielle Daten (oder alle Daten) in einer Patientenakte mit anderen Diensten auszutauschen., einschließlich teilnehmende Drittanbieter-Diensten, die Sie autorisieren. Kein Dienst hat einen Zugriff auf Ihre Daten über HealthVault, es sei denn, dass ein berechtigter Benutzer den Zugriff über HealthVault gewährt. HealthVault erlaubt Ihnen, den Zugriff durch Annahme oder Ablehnung von Anforderungen zu kontrollieren. Für jeden Dienst, dem Zugriff gewährt wird, wählen Sie aus, welche Gesundheitsinformationen in einer bestimmten Patientenakte ausgetauscht werden und welche Aktionen der einzelne Dienst mit den Gesundheitsinformationen vornehmen darf.

Ein Dienst, den Sie für eine Akte autorisieren, erhält den vollständigen Namen, der mit Ihrem HealthVault-Konto verbunden ist, den Spitznamen der autorisierten Akte (n) und Ihre Beziehung zu dieser Akte. Der Dienst wird weiterhin solange Zugang über HealthVault haben, bis Sie die Erlaubnis widerrufen. Microsoft kann den Zugang eines Dienstes zu HealthVault widerrufen, wenn dieser seine Datenschutzverpflichtungen gegenüber Microsoft nicht einhält. Außer der Beschränkung des Zugangs zu Ihren HealthVault-Daten kontrollieren oder überwachen wir jedoch diese Drittanbieterdienste nicht, und deren Datenschutzpraktiken unterscheiden sich möglicherweise.

Berichte an Gesundheitsdienstleister in den USA. In den Vereinigten Staaten ermöglichen wir teilnehmenden Gesundheitsdienstleistern den Erhalt von Berichten darüber, ob die Informationen, die sie an eine Akte in Microsoft Health-Diensten senden, verwendet werden. Diese Funktion unterstützt das Ziel der „vernünftigen Verwendung“ des HITECH-Gesetzes, das Gesundheitsdienstleistern Anreize gibt, ihren Patienten Kopien von deren medizinischen Informationen elektronisch zuzusenden. Dienstleister, die daran teilnehmen, können Berichte erhalten, die eine Nummer enthalten, die der Dienstleister verwenden kann, um den Patienten in seinem System zu identifizieren, und ob der Benutzer eine der „qualifizierenden Maßnahmen“ in HealthVault unternahm (aber keine Informationen, um welche Maßnahme es geht). Eine „Qualifizierende Maßnahme“ beinhaltet momentane Aktivitäten, wie z.B. Anzeigen, Herunterladen oder Übertragen von Gesundheitsinformationen über E-Mail. Sie können die Berichterstattung über Ihre Akten deaktivieren.

Zugriff und Steuerung. Sie können Ihre HealthVault-Kontodaten überprüfen, bearbeiten oder löschen, oder Ihr HealthVault-Konto jederzeit löschen. Nur Treuhänder können ein Element dauerhaft löschen. Wenn Sie eine Patientenakte löschen, wird sie bei allen Benutzern gelöscht, die darauf Zugriff hatten.

Beim Löschen Ihres HealthVault-Kontos löschen wir alle Akten, für die Sie der einzige Treuhänder sind. Wenn Sie den Treuhänderzugang für eine Akte austauschen, können Sie entscheiden, ob Sie die Akte löschen wollen. Microsoft wartet eine begrenzte Zeitdauer ab, bevor Ihre Daten permanent gelöscht werden, um ein versehentliches oder böses Entfernen Ihrer Gesundheitsdaten zu vermeiden.

HealthVault pflegt eine vollständige Historie jedes Zugriffs, jeder Änderung oder Löschung durch Benutzer oder Dienste, die das Datum, die Aktion und den Namen der Person oder des Dienstes enthält. Treuhänder der Akten können den Verlauf dieser Akten untersuchen.

E-Mail-Kommunikation. Wir verwenden die von Ihnen bei der Erstellung des Kontos angegebene E-Mail-Adresse, um Ihnen eine E-Mail zu senden, in der Sie aufgefordert werden, Ihre E-Mail-Adresse zu validieren, um diese in Einladungen zum Austausch, die Sie über HealthVault senden, einzufügen sowie Ihnen Dienstbenachrichtigungen zu senden, wie z.B. E-Mail-Benachrichtigungen darüber, dass Informationen vorliegen, die Ihren HealthVault-Akten hinzugefügt werden können.

HealthVault sendet regelmäßig Newsletter, um sie über die neuesten Verbesserungen zu informieren. HealthVault sendet Ihnen zudem regelmäßig eine E-Mail, die Ihre jüngsten Konto-Aktivitäten zusammenfasst. Vorbehaltlich Ihrer Kontakteinstellungen verwenden wir ebenfalls Ihre E-Mail-Adressen, um Ihnen E-Mail-Werbungen zuzusenden. Sie können das Abonnement dieser E-Mails jederzeit abbestellen.

- [So erreichen Sie uns](#)
- [Impressum](#)
- [Datenschutz und Cookies](#)
- [Nutzungsbedingungen](#)
- [Markenzeichen](#)
- [Informationen zu unserer Werbung](#)
- [EU Compliance DoCs](#)
- © Microsoft 2018