

Datenschutz Windows 10

Windows 10 analysiert verschiedene persönliche Daten. Verwendet werden Daten wie z.B. die E-Mail-Adresse und Inhalt der gesendeten und empfangenen E-Mails, persönliche Interessen und Favoriten, Einkäufe und Zahlungsdaten, das persönliche Adressbuch usw.

Viele dieser Daten werden auch an Microsoft übermittelt. Die meisten Mechanismen zur Datenübermittlung lassen sich jedoch ausschalten. Einerseits sollten bei der Installation (Update) von Windows 10 gewisse Punkte beachtet werden und andererseits können nachträglich noch diverse Einstellungen vorgenommen werden. Unsere Checkliste soll Ihnen helfen die richtigen Einstellungen vorzunehmen um Ihre Daten und privaten Informationen bestmöglich zu schützen.

Wir haben uns bemüht, eine möglichst allgemeingültige Checkliste für Privatanwendende zu verfassen. Dennoch können die einzelnen Konfigurationsmöglichkeiten und Einstellungen in besonderen Fällen abweichen. Die Checkliste bezieht sich auf die per **24. Mai 2019** verfügbaren Optionen.

Einstellungen während der Installation (Update) von Windows 10

Während der Installation (Update) von Windows 10 werden die verschiedenen Optionen der Datenschutzeinstellungen auf einer Seite mit dem Titel «Wählen Sie die Datenschutzeinstellungen für Ihr Gerät aus» angezeigt und bei jeder Einstellung transparent erklärt, wofür sie da ist. Standardmässig sind alle Einstellungen «Aktiviert».

Um zu verhindern, dass Windows zu viele Daten ungewollt an Microsoft sendet, sollten Sie alle Einstellungen auf «Deaktiviert» stellen.

Wenn Sie gewisse Einstellungen individualisieren und eventuell teilweise aktivieren möchten, warten Sie, bis Windows fertig installiert ist und nehmen Sie die Einstellungen dann vor.

Einstellungen nach der Installation (Update) von Windows 10

Sollten Sie Windows 10 bereits mit den Standardeinstellungen installiert (upgedatet) haben, können Sie die Einstellungen nachträglich in Windows anpassen. Sie finden das entsprechende Menü unter **Start > Einstellungen > Datenschutz**.

Allgemein

Um sich davor zu schützen, dass Ihr Gerät anhand einer von Windows vergebenen Werbe-ID eindeutig identifiziert werden kann, schalten Sie die erste Option aus.

Die zweite Option sollten Sie eingeschaltet lassen. So stellen Sie sicher, dass Websites unter Windows wo immer möglich in der in Windows eingestellten Systemsprache angezeigt werden.

Die dritte Option dient der lokalen Verbesserung von Windows und kann eingeschaltet sein. Apps, die Sie häufig starten, kann Windows so schneller bereitstellen.

Option	Unsere Empfehlung

Ermöglicht Apps die Verwendung der Werbe-ID, um Ihnen anhand Ihrer App-Aktivität interessantere Werbung anzuzeigen (bei Deaktivierung wird Ihre ID zurückgesetzt)	Aus
Websites den Zugriff auf die eigene Sprachliste gestatten, um die Anzeige lokal relevanter Inhalte zu ermöglichen	Ein
Windows erlauben, das Starten von Apps nachzuverfolgen, um Start und Suchergebnisse zu verbessern	Ein
Vorgeschlagene Inhalte in der Einstellungs-App anzeigen	Aus

Spracherkennung

Windows und die Sprachassistentin Cortana können Ihre Stimme analysieren und so persönliche Empfehlungen verbessern. Da dabei der Kalender, die Kontaktdaten und Ähnliches ausspioniert wird, sollten Sie diese Option ausschalten.

Freihand- und Eingabeanpassung

Windows und die Sprachassistentin Cortana können Ihre Handschrift analysieren und so persönliche Empfehlungen verbessern. Da dabei der Kalender, die Kontaktdaten und Ähnliches ausspioniert wird, sollten Sie diese Option ausschalten.

Diagnose und Feedback

Die Datensammlung von Microsoft lässt sich nicht ganz unterbinden. Sie haben die Wahl, ob Sie wenige oder viele Daten übermitteln möchten. Um möglichst wenige Daten zu übermitteln, wählen Sie «Standard» aus.

Option	Unsere Empfehlung
Freihand- und Eingabeerkennung verbessern	Aus
Individuelle Benutzererfahrung	Aus
Diagnosedaten anzeigen	Aus

Aktivitätsverlauf

Windows analysiert, mit welchen Anwendungen Sie gearbeitet haben und bietet Ihnen eine Historie Ihrer Aktivitäten an.

Mit einem Microsoft-Konto und aktivierter Cloud-Synchronisation können Sie so mit mehreren Geräten auf die gleiche Timeline zugreifen. Wenn Sie das nicht wollen, sollten Sie dies ausschalten.

Option	Unsere Empfehlung
Meinen Aktivitätsverlauf auf diesem Gerät speichern	Deaktiviert
Meinen Aktivitätsverlauf an Microsoft senden	Deaktiviert

Position

Die Positionserkennung sollte ausgeschaltet werden. Mit einem Klick auf «Löschen» können Sie den bisher gespeicherten Verlauf löschen.

Falls Sie einen GPS-Empfänger haben, können Sie bei Bedarf einzeln den installierten Apps die Berechtigung für

die Positionserkennung erteilen oder entziehen.

Option	Unsere Empfehlung
Zugriff auf den Standort auf diesem Gerät zulassen	Aus

Kamera

Hier kann verhindert werden, dass jede App automatisch Zugriff auf die Kamera hat. Schalten Sie diese Option aus.

Falls Sie über eine Kamera verfügen und einer App den Zugriff erlauben möchten, sollten Sie dies für jede einzelne App tun und jeder den Zugriff erteilen oder entziehen.

Option	Unsere Empfehlung
Zugriff auf die Kamera auf diesem Gerät zulassen	Aus

Mikrofon

Hier kann verhindert werden, dass jede App automatisch Zugriff auf das Mikrofon hat. Schalten Sie diese Option aus.

Falls Sie über ein Mikrofon verfügen und einer App den Zugriff erlauben möchten, sollten Sie dies für jede einzelne App tun und jeder den Zugriff erteilen oder entziehen.

Option	Unsere Empfehlung
Zugriff auf das Mikrofon auf diesem Gerät zulassen	Aus

Benachrichtigungen

Sie können allen Apps grundsätzlich den Zugriff auf Ihre Benachrichtigungen erlauben oder entziehen. Möchten Sie den Zugriff nicht generell unterbinden, können Sie für jede einzelne App den Zugriff erteilen oder entziehen. Der Zugriff sollte nur vertrauenswürdigen Apps erteilt werden.

Kontoinformationen

Da dieser Zugriff primär für personalisierte Werbung benötigt wird, empfiehlt es sich, diese Option auszuschalten.

Option	Unsere Empfehlung
Zugriff auf Kontoinformationen auf diesem Gerät zulassen	Aus

Kontakte

Sie können allen Apps grundsätzlich den Zugriff auf Ihre Kontakte erlauben oder entziehen. Möchten Sie den Zugriff nicht generell unterbinden, können Sie für jede einzelne App den Zugriff erteilen oder entziehen. Der Zugriff sollte nur vertrauenswürdigen Apps erteilt werden.

Kalender

Sie können allen Apps grundsätzlich den Zugriff auf Ihren Kalender erlauben oder entziehen. Möchten Sie den Zugriff nicht generell unterbinden, können Sie für jede einzelne App den Zugriff erteilen oder entziehen. Der Zugriff sollte nur vertrauenswürdigen Apps erteilt werden.

Anrufliste

Sie können allen Apps grundsätzlich den Zugriff auf Ihre Anrufliste erlauben oder entziehen. Möchten Sie den Zugriff nicht generell unterbinden, können Sie für jede einzelne App den Zugriff erteilen oder entziehen. Der Zugriff sollte nur vertrauenswürdigen Apps erteilt werden.

E-Mail

Sie können allen Apps grundsätzlich den Zugriff auf Ihre E-Mails erlauben oder entziehen. Möchten Sie den Zugriff nicht generell unterbinden, können Sie für jede einzelne App den Zugriff erteilen oder entziehen. Der Zugriff sollte nur vertrauenswürdigen Apps erteilt werden.

Aufgaben

Sie können allen Apps grundsätzlich den Zugriff auf Ihre Aufgaben erlauben oder entziehen. Möchten Sie den Zugriff nicht generell unterbinden, können Sie für jede einzelne App den Zugriff erteilen oder entziehen. Der Zugriff sollte nur vertrauenswürdigen Apps erteilt werden.

Messaging

Sie können allen Apps grundsätzlich den Zugriff auf Ihre Nachrichten (SMS oder MMS) erlauben oder entziehen. Möchten Sie den Zugriff nicht generell unterbinden, können Sie für jede einzelne App den Zugriff erteilen oder entziehen. Der Zugriff sollte nur vertrauenswürdigen Apps erteilt werden.

Funktechnik

Sie können allen Apps grundsätzlich den Zugriff auf Ihre Funktechnik (Bluetooth etc.) erlauben oder entziehen. Möchten Sie den Zugriff nicht generell unterbinden, können Sie für jede einzelne App den Zugriff erteilen oder entziehen. Der Zugriff sollte nur vertrauenswürdigen Apps erteilt werden.

Weitere Geräte

Ein automatischer Informationsaustausch, z.B. in einem öffentlichen WLAN, stellt ein erhebliches Sicherheitsrisiko dar. Schalten Sie diese Option deshalb aus.

Beachten Sie aber, dass kontaktloses Bezahlen mit dem Smartphone (bei Windows 10 Mobile) so nicht mehr möglich ist.

Option	Unsere Empfehlung
Mit nicht gekoppelten Geräten kommunizieren	Aus

Hintergrund-Apps

Als Hintergrund-Apps bezeichnet Microsoft Programme, die auch dann aktuell bleiben, wenn sie nicht aktiv genutzt werden. Indem Sie einer App dieses Recht entziehen, können Sie Strom sparen. Speziell auf mobilen Geräten entlastet das den Akku. Mit Datenschutz haben diese Einstellungen aber nichts zu tun. Sie können diese Option je nach Bedürfnis einstellen.

App-Diagnose

Auch die Apps übermitteln in den Standardeinstellungen viele Diagnosedaten an Microsoft. Es empfiehlt sich, diese Option auszuschalten.

Option	Unsere Empfehlung
Zugriff auf App-Diagnoseinformationen auf diesem Gerät zulassen	Aus

Automatische Dateidownloads

Ist gemäss Ihren obigen Einstellungen deaktiviert.

Dokumente

Sie können allen Apps grundsätzlich den Zugriff auf Ihre Dokumentbibliotheken erlauben oder entziehen. Möchten Sie den Zugriff nicht generell unterbinden, können Sie für jede einzelne App den Zugriff erteilen oder entziehen. Der Zugriff sollte nur vertrauenswürdigen Apps erteilt werden.

Bilder

Sie können allen Apps grundsätzlich den Zugriff auf Ihre Bildbibliotheken erlauben oder entziehen. Möchten Sie den Zugriff nicht generell unterbinden, können Sie für jede einzelne App den Zugriff erteilen oder entziehen. Der Zugriff sollte nur vertrauenswürdigen Apps erteilt werden.

Videos

Sie können allen Apps grundsätzlich den Zugriff auf Ihre Videobibliotheken erlauben oder entziehen. Möchten Sie den Zugriff nicht generell unterbinden, können Sie für jede einzelne App den Zugriff erteilen oder entziehen. Der Zugriff sollte nur vertrauenswürdigen Apps erteilt werden.

Dateisystem

Sie können allen Apps grundsätzlich den Zugriff auf alle Dateien, einschliesslich Ihrer Dokumente, Bilder, Videos und lokalen OneDrive-Dateien erlauben oder entziehen. Möchten Sie den Zugriff nicht generell unterbinden, können Sie für jede einzelne App den Zugriff erteilen oder entziehen. Der Zugriff sollte nur vertrauenswürdigen Apps erteilt werden.

Datenschutz-Dashboard

Um die Transparenz der gesammelten Daten zu gewährleisten, bietet Microsoft ein Datenschutz-Dashboard an, das alle gespeicherten Informationen auflistet. Diese können Sie auch löschen, sofern Sie mit einem Microsoft-Account angemeldet sind. Zum Datenschutz-Dashboard gelangen Sie über folgenden Link:

<https://account.microsoft.com/privacy> (<https://account.microsoft.com/privacy>)