Ihr PC-Sicherheits-Berater

So schützen Sie Ihre Privatsphäre und sensiblen Daten

3 Wechseln Sie zum lokalen Konto
Brauchen Sie das Microsoft-Konto nicht zwingend, speichern Sie Ihre Kontodaten aus Sicherheitsgründen lokal.

4 Weisen Sie Windows in seine Schranken
Legen Sie fest, welche Daten Windows 10 weitergeben darf, sonst haben Sie eine Datenschleuder.

6 Verrät Edge Daten über Sie an Microsoft?
Schieben Sie Microsoft einen Riegel vor und stellen Sie die Datenschutz-Einstellungen für Edge scharf.

7 Stoppen Sie die Bildschirmkopie-Dateien
Wussten Sie, dass Windows 10 Ihre Bildschirmkopien an Microsoft schickt? Schalten Sie diese Spionage aus.

So hindern Sie Microsoft ab sofort an der Datenspionage: Schalten Sie alle Datenübertragungen einfach ab

Schützen Sie sich vor der „Abhöranlage Windows 10"

Seit Windows 10 auf dem Markt ist, hat es herbe Kritik an diesem „sichersten Windows aller Zeiten" (Microsoft) gegeben.

Zuletzt wies das **B**undesamt für die **S**icherheit in der **I**nformationstechnik (BSI) Ende 2018 auf im Hintergrund übertragene Telemetriedaten hin.

Beim großen Windows-10-Update 19H1, das seit April 2019 zur Verfügung steht, werden Sie zwar nach Datenschutz-Einstellungen gefragt, doch das reicht nicht.

Meine Meinung: Die Abfragen sind eine Verschleierungstechnik. Folgen Sie meinen Anleitungen. Nur so sind Sie geschützt.

Viele Grüße, Ihr

Michael-Alexander Beisecker,
Deutschlands PC-Sicherheitsexperte Nr. 1

Kostenlose Experten-Hilfe:
Exklusiv für Sie als Abonnenten: Die Sofortauskunft mit zuverlässigen Antworten und professionellen Tipps direkt von der Redaktion.
Redaktions-Hotline: **Mittwoch zwischen 15.00 und 18.00 Uhr, Tel.: 02 08/69 07 977**

Überprüfen Sie alle Datenschutz-Einstellungen nach meinen Vorgaben

Mit nur 7 Aktionen schützen Sie sich vor der Windows-10-Spionage

Jedes größere Windows-10-Update bringt Veränderungen an den Datenschutz-Einstellungen. So auch das neue 19H1-Update: Es kommen Einstellungen hinzu, es werden Einstellungen umbenannt oder fallen ganz weg. Werden Sie daher jetzt nach dem 19H1-Update aktiv und überprüfen Sie Ihre Datenschutz-Einstellungen. Nur so stellen Sie sicher, dass von Windows 10 nur die Daten übertragen werden, die Sie Microsoft zur Verfügung stellen möchten.

Datenschutz klingt kompliziert, ist aber bei Windows 10 ganz einfach. Alle notwendigen Einstellungen lassen sich per Mausklick ausführen. Es gibt jedoch sehr viele dieser Einstellungen und nicht bei jeder ist sofort erkennbar, welche Datenübertragung dadurch unterbunden wird.

Damit Sie keine wichtige Einstellung übersehen und immer die richtige Funktion wählen, führe ich Sie Schritt für Schritt durch die notwendigen Aktionen. Das Übertragen der Telemetriedaten wird dabei nicht komplett unterdrückt, denn es gibt wichtige Daten, die etwa die Windows-10-Updates und die automatische Fehlerbehebung sicherstellen.

Mit diesen 7 Aktionen schränken Sie den Datenhunger von Windows 10 sinnvoll ein:

Datenschutz-Aktion 1:	Ändern Sie beim Windows-10-Update 19H1 die 5 Voreinstellungen von Microsoft ab (siehe Seite 2).
Datenschutz-Aktion 2:	Wechseln Sie zum lokalen Konto oder prüfen Sie die Synchronisierung (siehe Seite 3).
Datenschutz-Aktion 3:	Stellen Sie die Windows-Berechtigungen auf optimalen Datenschutz ein (siehe Seite 4).
Datenschutz-Aktion 4:	Beschränken Sie die Rechte der Apps (siehe Seite 4).
Datenschutz-Aktion 5:	Stellen Sie den Edge-Browser sicher ein (siehe Seite 6).
Datenschutz-Aktion 6:	Stoppen Sie das Abspeichern von Fotos im Internet (siehe Seite 7).
Datenschutz-Aktion 7:	Machen Sie die 4-Augen-Kontrolle mit dem Datenschutz-Tool O&O Shut Up (siehe Seite 8).

>>> Lesen Sie bitte weiter auf Seite 2

Datenschutz-Aktion 1: Ändern Sie beim Windows-10-Update 19H1 die 5 Voreinstellungen

Aufgrund der Proteste von Datenschützern und Regierungen fragt Microsoft beim Windows-10-Update 19H1 fünf Datenschutz-Einstellungen ab. Nehmen Sie hier die von mir empfohlenen Einstellungen vor, bevor Sie auf „Annehmen" klicken. Damit stellen Sie die Weichen für den Schutz Ihrer Privatsphäre, den Sie dann mit den Datenschutz-Aktionen 2 bis 7 immer weiter optimieren. Wurde das Update 19H1 bereits bei allen Ihren PCs durchgeführt, machen Sie gleich mit der Datenschutz-Aktion 2 weiter. Keine Sorge, Sie erreichen auch dann mit meinen Empfehlungen den bestmöglichen Schutz.

Während des 19H1-Updates werden Ihnen auf einer Bildschirmseite 5 voreingestellte Datenschutz-Einstellungen angeboten (a). Der Datenschutz ist ganz einfach: Klicken Sie auf die Schalter, deren Einstellung Sie ändern möchten.

Position: Hier fragt Microsoft ab, ob Windows 10 und die Apps Ihre Positionsdaten übermitteln dürfen. Das kann bei einem Notebook-PC oder Tablet sinnvoll sein, wenn Sie den Mobilrechner zum Beispiel auch zu Navigationszwecken nutzen oder auf automatisch bezogene Standort-Informationen wie das örtliche Wetter Wert legen.

Meine Empfehlung: Stellen Sie die Positionsdaten-Übermittlung bei einem Desktop-PC auf **Aus**. Sofern Sie die Standort-Übermittlung bei Ihren Mobilrechnern nicht benötigen, sollten Sie sie auch dort abschalten. Andernfalls lassen Sie den Schalter auf **Aktiviert**. Um den Schalter „umzulegen", klicken Sie ihn einfach an: Ist der Schalter blau, ist er aktiviert. Ist der Schalter grau, ist er deaktiviert.

Spracherkennung: Windows 10 kann Sie mit der Sprachassistentin Cortana und seit dem Update 19H1 auch mit Alexa von Amazon unterstützen. Doch dazu geben Sie Microsoft die Zustimmung, alle Ihre Gespräche zu belauschen und an Microsoft-Server bzw. Amazon-Server zur Auswertung zu übertragen. Zusätzlich lässt sich die Spracherkennung womöglich durch unbefugte Personen missbrauchen.

Meine Empfehlung: Stellen Sie die Spracherkennung auf **Aus**, wenn Sie diese nicht verwenden.

Diagnose: Windows 10 überträgt im Hintergrund ständig eine Vielzahl von Telemetriedaten an Microsoft-Server im Internet. Diese Daten sind laut Microsoft erforderlich, um auftretende Fehler zu bereinigen, wichtige Updates zu installieren und Sie zu unterstützen. Microsoft erfährt über diese Daten aber auch ganz genau, wann Sie sich bei Ihrem Windows 10 anmelden, wie lange Sie es nutzen und welche Programme Sie verwenden.

Meine Empfehlung: Wählen Sie bei **Diagnose** per Klick die Einstellung **Einfach**. Sie unterbinden die Datenübertragung damit nicht vollständig, senken sie jedoch auf ein erträgliches Maß und können später weitere Maßnahmen ergreifen, wenn Sie möchten.

Individuelle Benutzererfahrung mit Diagnosedaten: Microsoft lockt hier mit dem Versprechen von Praxis-Tipps und Empfehlungen, wenn Sie dafür Ihre Diagnosedaten freigeben.

Meine Empfehlung: Stellen Sie den Schalter auf **Aus**, denn sonst hebeln Sie die Einstellung bei **Diagnose** wieder aus und Microsoft erhält praktisch über die Hintertür weiter große Mengen an Diagnosedaten.

Relevante Werbeanzeigen: Windows 10 blendet Werbeanzeigen ein. Über diese Werbung erhält Microsoft Einnahmen. Die Werbung lässt sich durch Auswerten Ihrer Daten an Ihre Interessen anpassen. Dazu sind Werbe-IDs (Kennzeichen) erforderlich. Sie werden daher gefragt, ob Sie den Werbe-IDs zustimmen.

Meine Empfehlung: Stellen Sie den Schalter auf **Aus**, denn die Werbe-IDs beeinträchtigen Ihre Privatsphäre und fördern das Anzeigen von Werbung in Windows 10.

Die voreingestellten Datenschutz-Einstellungen sollten Sie nicht einfach übernehmen, denn dann erhält Microsoft vollen Datenzugriff.

Fazit: Folgen Sie bei diesen 5 Abfragen meinen Datenschutz-Empfehlungen. Damit verhindern Sie zwar nicht die Datenübertragung bei Windows 10, aber es ist ein erster Anfang gemacht. Das Feintuning und Beseitigen der restlichen unerwünschten Datenspionage-Attacken steuern Sie über die folgenden Datenschutz-Aktionen 2 bis 7.

Datenschutz-Aktion 2: Wechseln Sie zum lokalen Konto oder prüfen Sie die Synchronisierung

Haben Sie Windows 10 entsprechend den Microsoft-Vorgaben eingerichtet, dann melden Sie sich über Ihr Microsoft-Konto bei Ihrem Windows an. Dadurch haben Sie praktische Vorteile: Ihre Windows-Einstellungen werden voreingestellt über alle Ihre Windows-PCs synchronisiert, Ihnen steht der Online-Speicher OneDrive zur Verfügung und Microsoft merkt sich Ihre Windows- und Office-Lizenzen. Doch das Microsoft-Konto hat den Nachteil, dass Microsoft dort alle Informationen über Sie sammeln und Ihnen personenbezogen zuordnen kann. Durch einen Wechsel zur lokalen Anmeldung können Sie Ihre Privatsphäre vor Microsoft schützen.

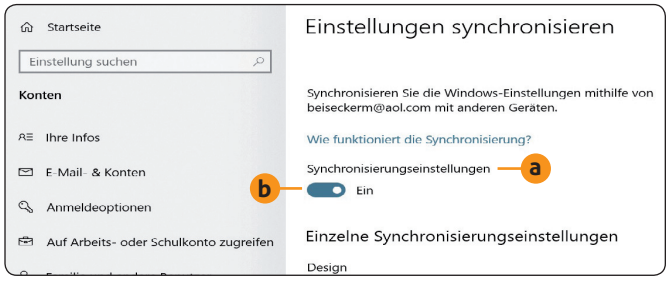
Stellen Sie auf das lokale Konto um:

1. Öffnen Sie mit ⊞+I die **Windows-Einstellungen**.
2. Wählen Sie **Konten**.
3. Schauen Sie auf der rechten Seite nach, ob dort eine E-Mail-Adresse unter Ihrem Namen angegeben ist. Dann sind Sie per Microsoft-Konto angemeldet. Haben Sie dagegen bereits eine lokale Anmeldung, brechen Sie diese Anleitung ab und machen Sie mit Datenschutz-Aktion 3 ab Seite 4 weiter.
4. Klicken Sie auf **Stattdessen mit einem lokalen Konto anmelden** und geben Sie Ihr aktuelles Windows-Kennwort zur Bestätigung ein.
5. Vergeben Sie einen Benutzernamen für Ihr neues lokales Konto und ein sicheres Kennwort (mindestens 16 Zeichen, bestehend aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen).
6. Bestätigen Sie das Anlegen des lokalen Kontos mit **Abmelden und fertig stellen**.
7. Starten Sie Ihren PC neu und melden Sie sich lokal an. Bitte beachten Sie, dass Änderungen am Hintergrundbild und sonstigen Windows-Einstellungen jetzt nicht mehr automatisch bei allen Ihren Windows-10-PCs übernommen werden. Möchten Sie OneDrive nutzen, müssen Sie sich separat mit Ihrem Microsoft-Konto anmelden.

Halten Sie am Microsoft-Konto fest, prüfen Sie die Synchronisierungs-Einstellungen

Kommt ein lokales Konto für Sie nicht infrage, weil Sie die Vorteile des Microsoft-Kontos nicht missen möchten, dann sollten Sie zumindest die Synchronisierungs-Einstellungen überprüfen:

1. Öffnen Sie mit ⊞+I die **Windows-Einstellungen**.
2. Wählen Sie **Konten** und **Einstellungen synchronisieren**.
3. Wünschen Sie generell keine Synchronisierung, dann schalten Sie **Synchronisierungseinstellungen** (a) auf **Aus**. Alternativ wählen Sie bei den 5 Schaltern darunter (b), welche Einstellungen Sie synchronisieren möchten und welche nicht.



Die Synchronisierung ist praktisch, wenn Sie mehrere PCs nutzen, beispielsweise einen Desktop-PC und ein Notebook.

Meine Empfehlung: Entscheiden Sie nach Ihrem Arbeitsumfeld, ob Sie sich lokal anmelden oder nicht:

- Legen Sie höchsten Wert auf Datenschutz und nutzen weder Online-Speicher noch Office 365 (Online-Office von Microsoft), dann ist das lokale Konto für Sie ideal.
- Benötigen Sie dagegen ständig Online-Speicher und wechseln häufig zwischen Ihren PCs, dann kommen Sie um die Anmeldung per Microsoft-Konto nicht herum. Ein lokales Konto wäre viel zu unpraktisch, da Sie manuell synchronisieren und sich ständig online anmelden müssten.

Benötigen Sie Entscheidungshilfe, rufen Sie bei der Redaktions-Hotline an (siehe Seite 1) oder fragen mich über den Computerwissen Club: https://club.computerwissen.de.

LESERSERVICE

Redaktionshilfe: Fragen Sie bei Sicherheitsbedenken immer zuerst Ihren persönlichen PC-Sicherheits-Berater Michael-Alexander Beisecker.

Melden Sie sich dazu einfach kostenlos unter **https://club.computerwissen.de** an und stellen Sie ihm dort Ihre Fragen. **Michael-Alexander Beisecker** und seine Redaktionsmitarbeiter helfen Ihnen gern weiter. Sie erhalten werktags innerhalb von 48 Stunden eine Antwort auf Ihre Frage – garantiert.

Datenschutz-Aktion 3: Stellen Sie die Windows-Berechtigungen auf optimalen Datenschutz ein

Sie haben in den beiden Datenschutz-Aktionen 1 und 2 besondere Fälle der Datenschutz-Einstellungen kennengelernt, die im ersten Fall nur bei der Update-Installation erscheinen und im zweiten Fall zu den Kontoeinstellungen gehören. In Datenschutz-Aktion 3 und 4 geht es jetzt um den Kern der Datenschutz-Einstellungen. Diese Einstellungen sind unterteilt in die Windows-Berechtigungen und die App-Berechtigungen. Zunächst überprüfen Sie die Windows-Berechtigungen, die übergeordnet für das gesamte Windows gelten.

Mit diesen 7 Einstellungen im Register **Diagnose und Feedback** geben Sie nur das Minimum an Daten preis:

1. Öffnen Sie mit ⊞+I die **Windows-Einstellungen** und wählen Sie **Datenschutz**. Das Register **Allgemein** ist voreingestellt geöffnet.
2. Schalten Sie **Ermöglicht Apps die Verwendung der Werbe-ID** … auf **Aus**, um das Anzeigen speziell an Ihre Interessen angepasster Werbung zu unterbinden.
3. Schalten Sie **Windows erlauben, das Starten von Apps nachzuverfolgen** auf **Aus**. Denn wenn Sie Windows diese Überwachung erlauben, dann erfährt auch Microsoft genau, was Sie tun.
4. Wechseln Sie zum Register **Spracherkennung**. Schalten Sie **Online-Spracherkennung** auf **Aus**, sofern Sie die Spracheingabe nicht für Cortana oder das Diktieren verwenden.
5. Wechseln Sie zum Register **Freihand- und Eingabeanpassung**. Schalten Sie **Mich kennenlernen** auf **Aus**, sofern Ihr PC keinen berührungsempfindlichen Bildschirm hat oder Sie keine handschriftlichen Eingaben auf dem Bildschirm tätigen.
6. Wechseln Sie zum Register **Diagnose und Feedback**. Nehmen Sie die Einstellungen entsprechend der nachfolgenden Tabelle vor.

Bezeichnung der Einstellung	Meine empfohlene Einstellung
Diagnosedaten	Standard
Freihand- und Eingabe verbessern	Aus
Individuelle Benutzererfahrung	Aus
Diagnosedaten anzeigen	Aus
Diagnosedaten löschen	Löschen (regelmäßig einmal im Monat)
Feedbackhäufigkeit	Automatisch (empfohlen)
Empfohlene Problembehandlung	Vor dem Beheben von Problemen fragen

7. Wechseln Sie zum Register **Aktivitätsverlauf**. Stellen Sie **Meinen Aktivitätsverlauf an Microsoft senden** auf **Aus**.

Meine Empfehlung: Überprüfen Sie die Windows-Berechtigungen und nehmen Sie alle Einstellungen wie von mir empfohlen vor. Das ist ganz einfach: Sie brauchen den betreffenden Schalter nur anzuklicken, damit er seine Einstellung und Farbe ändert.

Datenschutz-Aktion 4: Beschränken Sie die Rechte der Apps

Nachdem Sie in der Datenschutz-Aktion 3 die Windows-Berechtigungen festgelegt haben, wenden Sie sich jetzt den App-Berechtigungen zu. Bei Windows 10 haben die Apps (Programme) voreingestellt sehr weit gehende Rechte und können zum Beispiel auf alle Kontakte, Termine, den Standort, die Kamera und das Mikrofon zugreifen, wenn Sie es nicht unterbinden. Daher sind die folgenden Einstellungen ganz besonders wichtig. Lassen Sie sich nicht von der großen Anzahl der Einstellungen abhalten und brechen Sie die Einstellung auch nicht auf halbem Weg ab, denn dann wäre ein Teil Ihrer Daten praktisch Freiwild für Microsoft und die App-Hersteller. Gehen Sie genau nach meiner Anleitung vor, werden Sie von Ihren genutzten Apps nicht verraten!

Einstellungs-Tipp: Alle Einstellungen laufen nach demselben Schema ab. Entweder Sie klicken wie in Datenschutz-Aktion 3 einfach auf den betreffenden Schalter oder es ist eine Schaltfläche **Ändern** vorhanden, über die Sie zum betreffenden Schalter gelangen.

Ich zeige Ihnen die ersten Einstellungen Schritt für Schritt und dann nehmen Sie die restlichen Einstellungen entsprechend der nachfolgenden Tabelle vor. Alle hier erläuterten Funktionen finden Sie in den **Einstellungen** bei **Datenschutz** unter **App-Berechtigungen**.

In nur 5 Schritten schalten Sie die Positionserkennung (Standortübertragung durch Apps) aus

1. Öffnen Sie mit ⊞+I die **Windows-Einstellungen** und wählen Sie **Datenschutz**.
2. Wechseln Sie zum Register **Position**.
3. Steht auf der rechten Seite **Die Positionserkennung ist für dieses Gerät eingeschaltet**, klicken Sie darunter auf **Ändern**. Stellen Sie den Schalter für **Zugriff auf die Position für dieses Gerät** auf **Aus**.
4. Klicken Sie unter **Positionsverlauf auf diesem Gerät löschen** auf **Löschen**.
5. Stellen Sie den Schalter für **Zulassen, dass Apps auf Ihren Standort zugreifen** auf **Aus**, wenn Sie keine Apps verwenden, die den Standort benötigen.

Entscheiden Sie sich in Schritt 3 dazu, die Positionserkennung eingeschaltet zu lassen, stellen Sie unter **Auswählen, welche Apps auf Ihren exakten Standort zugreifen können** den Schalter nur für die Apps auf **Ein**, die den Standort wirklich benötigen. Dazu gehört zum Beispiel eine Navigations- oder Wetter-App.

In der nachfolgenden Tabelle finden Sie meine empfohlenen Einstellungen für den Standardfall:

Register	Bezeichnung der Einstellung	Meine empfohlene Einstellung
Kamera	Zugriff auf die Kamera auf diesem Gerät zulassen	**Zugriff auf die Kamera für dieses Gerät** über **Ändern** auf **Aus**
	Zulassen, dass Apps auf Ihre Kamera zugreifen	**Aus**
	Zulassen, dass Desktop-Apps auf die Kamera zugreifen	**Aus**
Mikrofon	Zugriff auf das Mikrofon auf diesem Gerät zulassen	**Zugriff auf das Mikrofon für dieses Gerät** über **Ändern** auf **Aus**
	Zulassen, dass Apps auf Ihr Mikrofon zugreifen	**Aus**
	Desktop-Apps den Zugriff auf Ihr Mikrofon erlauben	**Aus**
Stimmaktivierung	Verwenden der Stimmaktivierung durch Apps zulassen	**Aus**
	Apps können auf Stimmaktivierung reagieren, wenn dieses Gerät gesperrt ist	**Aus** (wichtige Sicherheitseinstellung, um Hacker am Missbrauch der Sprachsteuerung und des Sprachassistenten zu hindern)
	Cortana soll auf das Schlüsselwort „hey cortana" reagieren	**Aus**
	Cortana auch bei gesperrtem Gerät verwenden	**Aus**
Benachrichtigungen	Zugriff auf Benutzerbenachrichtigungen auf diesem Gerät zulassen	**Zugriff auf Benutzerbenachrichtigung für dieses Gerät** über **Ändern** auf **Aus**
	Zugriff auf Benachrichtigungen durch Apps zulassen	**Aus**
Kontoinformationen	Zugriff auf Kontoinformationen auf diesem Gerät zulassen	**Zugriff auf Kontoinformationen für dieses Gerät** über **Ändern** auf **Aus**
	Zugriff auf Ihre Kontoinformationen durch Apps zulassen	**Aus**
Kontakte	Zugriff auf Kontakte auf diesem Gerät zulassen	**Kontaktzugriff für dieses Gerät** über **Ändern** auf **Aus**
	Zulassen, dass Apps auf Ihre Kontakte zugreifen	**Aus**
Kalender	Zugriff auf Kalender auf diesem Gerät zulassen	**Kalenderzugriff für dieses Gerät** über **Ändern** auf **Aus**
	Zulassen, dass Apps auf Ihren Kalender zugreifen	**Aus**
Telefonanrufe	Telefonanrufe auf diesem Gerät zulassen	**Zugriff auf die Anrufe für dieses Gerät** über **Ändern** auf **Aus**
	Apps dürfen Telefonanrufe ausführen	**Aus**
Anrufliste	Zugriff auf den Anrufverlauf auf diesem Gerät zulassen	**Anruflistenzugriff für dieses Gerät** über **Ändern** auf **Aus**
	Zugriff auf Ihren Anrufverlauf durch Apps zulassen	**Aus**
E-Mail	Zugriff auf E-Mail auf diesem Gerät zulassen	**E-Mail-Zugriff für dieses Gerät** über **Ändern** auf **Aus**
	Zulassen, dass Apps auf Ihre E-Mail zugreifen	**Aus**
Aufgaben	Zugriff auf Aufgaben auf diesem Gerät zulassen	**Aufgaben-Zugriff für dieses Gerät** über **Ändern** auf **Aus**
	Zulassen, dass Apps auf Ihre Aufgaben zugreifen	**Aus**
Messaging	Zugriff auf Messaging auf diesem Gerät zulassen	**Nachrichtenzugriff für dieses Gerät** über **Ändern** auf **Aus**
	Zulassen, dass Apps Nachrichten lesen oder senden	**Aus**
Funktechnik	Zugriff auf Funktechnik auf diesem Gerät zulassen	**Zugriff auf Steuerungen der Funktechnik für dieses Gerät** über **Ändern** auf **Aus**

Register	Bezeichnung der Einstellung	Meine empfohlene Einstellung
	Zulassen, dass Apps die Funktechnik des Geräts steuern	Aus
Weitere Geräte	Mit nicht gekoppelten Geräten kommunizieren	Aus
Hintergrund-Apps	Ausführen von Apps im Hintergrund zulassen	Aus
App-Diagnose	Zugriff auf App-Diagnoseinformationen auf diesem Gerät zulassen	Zugriff auf App-Diagnoseinformationen für dieses Gerät über Ändern auf Aus
	Apps den Zugriff auf Diagnoseinformationen über Ihre anderen Apps erlauben	Aus
Automatische Dateidownloads	Automatische Dateidownloads	Nicht zulassen
Dokumente	Zugriff auf Dokumentbibliotheken auf diesem Gerät zulassen	Dokumentbibliothekszugriff für dieses Gerät über Ändern auf Aus
	Apps den Zugriff auf Ihre Dokumentbibliothek erlauben	Aus
Bilder	Zugriff auf Bildbibliotheken auf diesem Gerät zulassen	Bildbibliothekszugriff für dieses Gerät über Ändern auf Aus
	Apps den Zugriff auf Ihre Bildbibliothek erlauben	Aus
Videos	Zugriff auf Videobibliotheken auf diesem Gerät zulassen	Videobibliothekszugriff für dieses Gerät über Ändern auf Aus
	Apps den Zugriff auf Ihre Videobibliothek erlauben	Aus
Dateisystem	Zugriff auf das Dateisystem auf diesem Gerät zulassen	Dateisystemzugriff für dieses Gerät über Ändern auf Aus
	Zulassen, dass Apps auf Ihr Dateisystem zugreifen	Aus

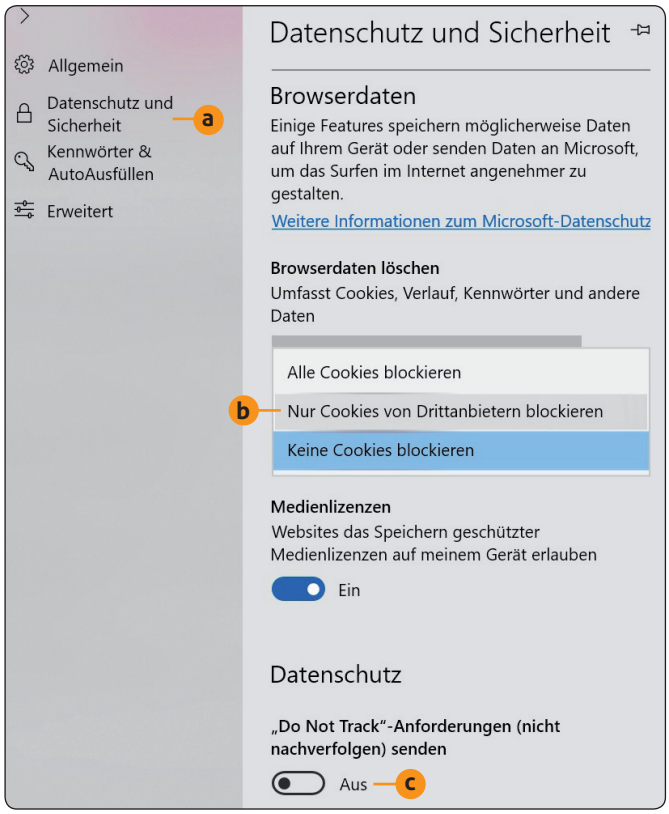
Die von mir empfohlenen Einstellungen für den Standardfall, dass keine Apps unter Windows 10 genutzt werden und Sie daher sämtliche Zugriffe aus Sicherheitsgründen deaktivieren.

Meine Empfehlung: Haben Sie alle Einstellungen entsprechend meinen Empfehlungen vorgenommen, haben Ihre Apps keinerlei Zugriffsrechte mehr, nicht einmal mehr auf das Dateisystem. Solange Sie keine Apps nutzen, stellt das kein Problem dar und ist eine Sicherheitsvorkehrung. Treten beim Verwenden von Apps Fehler auf, passen Sie die Einstellungen an: So braucht zum Beispiel Skype den Zugriff auf Mikrofon und Kamera, damit Sie Videotelefonate über das Internet durchführen können, und den Zugriff auf Ihre Kontakte, damit Sie diese anwählen können.

Datenschutz-Aktion 5: Stellen Sie den Edge-Browser sicher ein

Sie haben mit den Datenschutz-Aktionen 1 bis 4 alle Datenschutz-Einstellungen für Windows 10 und die Windows-Apps vorgenommen. Der zu Windows 10 gehörende Edge-Browser führt jedoch, was Daten angeht, ein Eigenleben, das Sie auch unter Ihre Kontrolle bringen sollten. Die Windows-Suche und die Sprachassistentin Cortana zeigen ihre Suchergebnisse immer über Microsoft Edge an. Dabei wird die Suchmaschine Bing von Microsoft verwendet. Jede Suche über Edge führt damit zu mehr Informationen für Microsoft über Sie, die Sie soweit möglich regelmäßig löschen sollten. Wie Sie dies bewerkstelligen, zeige ich Ihnen im Folgenden.

1. Klicken Sie rechts oben in Edge auf die **Menü**-Schaltfläche mit den drei Punkten ··· und wählen Sie **Einstellungen**. Das Register **Allgemein** wird geöffnet (siehe Bild auf der Folgeseite).
2. Stellen Sie bei **Neue Tabs öffnen mit** auf **Leere Seite** um. Microsoft analysiert sonst Ihr Surfverhalten.
3. Klicken Sie links in der Navigationsleiste auf **Datenschutz und Sicherheit** a.
4. Löschen Sie die gespeicherten Browser-Daten. Dazu klicken Sie auf **Zu löschendes Element auswählen** und setzen einen Haken vor alle Optionen von **Browserverlauf** bis **Kennwörter**. Dann klicken Sie auf **Löschen**.
5. Klicken Sie erneut links auf **Datenschutz und Sicherheit** und wählen Sie bei **Cookies** die Einstellung **Nur Cookies bei Drittanbietern blockieren** b. Damit hindern Sie Werbenetzwerke daran, Sie über die besuchten Webseiten durch das Internet zu verfolgen.
6. Stellen Sie **„Do Not Track"-Anforderungen (nicht nachverfolgen) senden** auf **Ein** c. Klicken Sie auf **Bing-Suchverlauf löschen**, wenn Sie die Liste der gesuchten Webseiten löschen möchten.
7. Stellen Sie den Schalter bei **Seitenvorhersage verwenden** auf **Aus**, da für diese Funktion die Adressen aller besuchten Webseiten an Microsoft übertragen werden.



Datenschützer empfehlen, auch **Windows Defender SmartScreen** auf **Aus** zu stellen. Ich rate Ihnen aus Sicherheitsgründen, dass Sie **Windows Defender SmartScreen** eingeschaltet lassen. Ganz egal, ob Sie diese Funktion nutzen, Microsoft erfährt ohnehin, welche Webseiten Sie besuchen. Sie werden aber auch vor gefährlichen Webseiten gewarnt, und das ist eine sehr wichtige Schutzfunktion.

Fazit: Edge ist für wichtige Windows-Funktionen wie die Sprachassistentin Cortana und die Windows-Suche der Standard-Browser. Daher sammelt Microsoft über diesen Browser bei ahnungslosen Anwendern sehr viele Daten ein. Mit den hier vorgestellten Datenschutz-Einstellungen für Edge schieben Sie Microsoft einen Riegel vor und schützen sich vor dem Ausspähen der besuchten Webseiten.

*In diesem Ausschnitt des Registers **Datenschutz und Sicherheit** von Edge sperren Sie Cookies von Drittanbietern.*

Datenschutz-Aktion 6: Stoppen Sie das Abspeichern von Fotos im Internet

Sie haben bei der Datenschutz-Aktion 5 gesehen, wie Sie den Datenschutz bei Edge sicherstellen. Doch es gibt noch mehr zu tun: Erstellen Sie mit Windows 10 eine Bildschirmkopie, wird diese automatisch auf Ihrem PC abgespeichert und über den Online-Speicherdienst OneDrive auf einen Microsoft-Server im Internet übertragen. Schließen Sie ein Smartphone, eine Digitalkamera oder eine Videokamera an Ihren PC an, werden auch die damit aufgenommenen Fotos und Videos an Microsoft gesendet. Was Microsoft mit diesen Fotos und Videos macht, ist nicht bekannt. Unterbinden Sie daher zur Sicherheit mit meiner folgenden Anleitung das Abspeichern im Internet.

In nur 5 Schritten schieben Sie der automatischen Foto-Abspeicherung ein für alle Mal gekonnt einen Riegel vor:

1. Öffnen Sie den Info-Bereich ganz rechts in der Taskleiste und klicken Sie das **OneDrive**-Symbol mit der rechten Maustaste an.
2. Wählen Sie **Einstellungen**.
3. Wechseln Sie zum Register **Automatisch speichern** a.
4. Entfernen Sie den Haken vor der Option **Fotos und Videos automatisch auf OneDrive speichern, wenn ich eine Kamera, ein Smartphone oder anderes Gerät an meinen PC anschließe** b.
5. Entfernen Sie den Haken vor der Option **Erstellte Screenshots automatisch auf OneDrive speichern** c und klicken Sie auf **OK**.

Impressum

Ihr PC-Sicherheits-Berater, ISSN 2196-9299

Dieses monothematische Supplement „Ihr Leitfaden zum Schutz Ihrer Privatsphäre unter Windows 10" gehört zu dem Titel „Ihr PC-Sicherheits-Berater".

Computerwissen, ein Verlagsbereich der VNR Verlag für die Deutsche Wirtschaft AG

Vorstand: Richard Rentrop

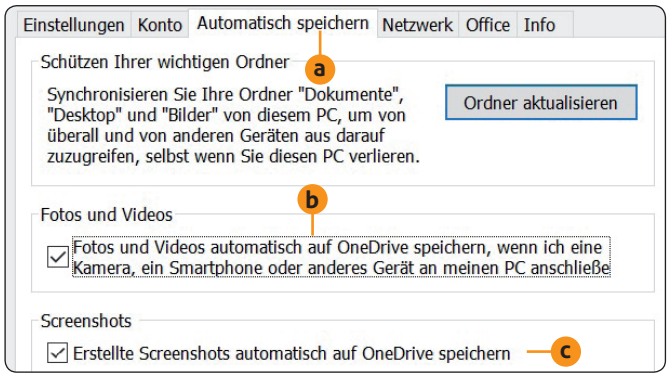
Chefredakteur: Michael-Alexander Beisecker (V.i.S.d.P.), Oberhausen

Herausgeberin: Patricia Sparacio

Adresse: Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Str. 2-4, 53177 Bonn

Telefon: 0228/9550190, Fax: 0228/3696350

Eingetragen: Amtsgericht Bonn HRB 8165



Fazit: Sie wissen nun, dass Microsoft automatisch Ihre Bildschirmkopien und Fotos erhält, wenn Sie die Einstellungen nicht ändern. Und Sie kennen den Weg, wie Sie Microsoft daran hindern.

Mit diesen beiden Einstellungen verhindern Sie, dass Ihre Bildschirmfotos, Fotos und Videos im Internet gespeichert werden.

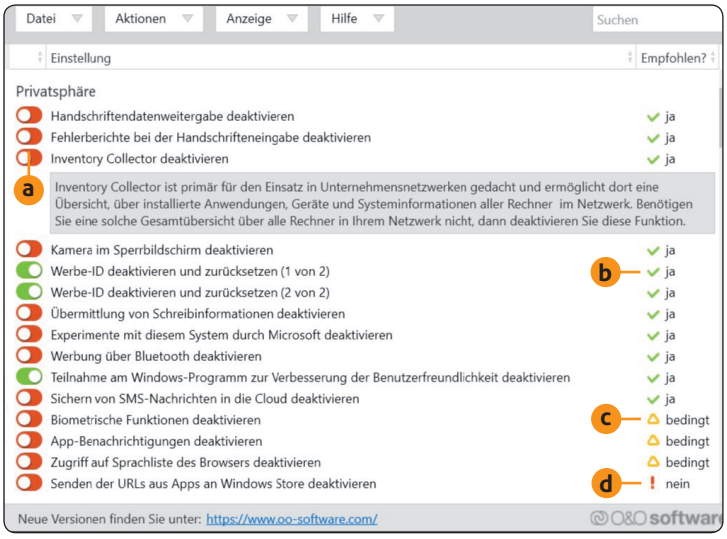
Datenschutz-Aktion 7: Machen Sie die 4-Augen-Kontrolle mit dem Datenschutz-Tool O&O ShutUp10

Sie haben in den Datenschutz-Aktionen 1 bis 6 die vielen verschiedenen Datenschutz-Einstellungen von Windows 10 kennengelernt und die empfohlenen Einstellungen vorgenommen. Machen Sie jetzt noch eine Abschlusskontrolle und prüfen Sie, ob es noch Datenlecks gibt, die Sie schließen möchten. Dazu empfehle ich Ihnen die mobile Version des kostenlosen Tools O&O ShutUp10 im Sinne einer 4-Augen-Kontrolle. Dieses Tool ändert Ihre Windows-Installation nicht und kann daher ganz einfach und rückstandsfrei wieder entfernt werden, wenn Sie es nicht mehr benötigen.

1. Laden Sie mit wenigen Mausklicks über den Link https://www.oo-software.com/de/shutup10 herunter.
2. Zeigt Ihr Browser das Tool nicht sofort an, öffnen Sie mit Strg+J die Download-Liste. Starten Sie das heruntergeladene Programm **OOSU10.exe** und bestätigen Sie der Benutzerkontenführung das Ausführen. Es erfolgt keine Installation, denn das Tool ist sofort betriebsbereit.
3. Der Schalter auf der linken Seite a zeigt Ihnen an, ob die jeweilige Option aktiviert ist oder nicht: Ist der Schalter rot, besteht kein Datenschutz. Ist der Schalter grün, überträgt Windows 10 die betreffenden Daten nicht.
4. Finden Sie in der Spalte **Empfohlen?** auf der rechten Seite einen grünen Haken b, wird das Aktivieren der Option von dem Tool empfohlen. Im Fall eines gelben Dreiecks c ist das Aktivieren nicht in jedem Fall ratsam; bei einem roten Ausrufezeichen d sollte die Option nicht aktiviert werden.
5. Blättern Sie alle Einträge durch und entscheiden Sie, ob Sie Änderungen vornehmen oder nicht.

Die Vorgaben des Tools sind nicht verbindlich, denn der Programm-Hersteller kann schließlich Ihr PC-System und Ihre Anforderungen an den Datenschutz nicht kennen. Letztendlich ist es Ihre Entscheidung, welche Datenübertragungen Sie zulassen und welche nicht.

Einfache Hilfe: Ist Ihnen die Bedeutung einer Einstellung bzw. eines Begriffs nicht klar, dann klicken Sie einfach auf den Eintrag und Sie erhalten eine Erklärung auf grauem Hintergrund angezeigt. Im Bild unten ist zum Beispiel die Beschreibung für **Inventory Collector deaktivieren** zu sehen.



O&O ShutUp zeigt Ihnen auf einen Blick für alle Datenschutz-Optionen, ob diese aktiviert sind und ob das Aktivieren vom Tool empfohlen wird oder nicht.

Für Ihre Sicherheit: Sie haben Windows 10 nun sicher eingestellt, sodass Ihre Daten und Ihre Privatsphäre geschützt sind. Meine Mitarbeiter aus der Redaktion und ich beantworten Ihnen gerne Ihre Fragen zu den Datenschutz-Einstellungen von Windows 10 über die Redaktions-Hotline und den Computerwissen Club: https://club.computerwissen.de.