

Inhaltsverzeichnis

Windows-Datenschutz-Checkliste	6
---	----------

1. Datenschutz von Anfang an	8
---	----------

Microsoft-Konto vs. lokale Anmeldung	8
Lokales Konto schon bei der Installation	9
Sonderfall Windows 10 Home	11
Datenschutzeinstellungen während der Installation	12
Microsoft-Konto auf lokale Anmeldung umstellen	17
Weitere lokale Konten anlegen	19
Microsoft-Konto nur in einzelnen Apps	21

2. Kontrolle über Ihre Daten	23
---	-----------

Diese Daten erfasst Microsoft über Sie	23
Telemetrie im Diagnostic Data Viewer überwachen	25
Was Ihr Microsoft-Konto synchronisiert	29
Das Profilbild Ihres Microsoft-Kontos	31
Das Windows-Insider-Programm	31

3. Datenschutzeinstellungen in Windows 10	34
--	-----------

Allgemeine Datenschutzoptionen	34
Diagnose und Feedback begrenzen	38
Das Übertragen von Telemetrie ganz blockieren	42
Aktivitätsverlauf	44
Position	46
Kamera	52

Mikrofon	55
Stimmaktivierung	57
Benachrichtigungen	60
Kontoinformationen	61
Kontakte	63
Kalender	65
Telefonanrufe	67
Anrufliste	68
E-Mail	70
Aufgaben	72
Messaging	74
Funktechnik	75
Weitere Geräte	77
Hintergrund-Apps	79
App-Diagnose	80
Automatische Dateidownloads	82
Dokumente, Bilder, Videos und Dateisystem	83
Datenschutzlücken auf dem Sperrbildschirm schließen	84

4. Weitere Windows-Apps und -Funktionen 88

Websuche im Startmenü deaktivieren	88
Windows-Sicherheit zum Datensparer machen	90
Erweiterte Zwischenablage mit Verlauf	93
Datenschützers Albtraum: Cortana	95
Die Skype-App vertraulich nutzen	101

5. Datenschutz im Edge-Browser 104

Globale Datenschutzeinstellungen in Edge	104
Websitespezifische Datenschutzeinstellungen	111
Unerwünschtes Tracking beim Websurfen verhindern	118
Im InPrivate-Modus ganz anonym surfen	121
Mit wechselnden Benutzerprofilen surfen	123
Lästige Benachrichtigungen von Webseiten blockieren	125
Mit dem Application Guard noch sicherer surfen	125
Browser-Erweiterungen für mehr Datenschutz	127
Sichere Webseiten mit HTTPS	134
Browserdaten löschen	141

6. Daten sicher mit anderen austauschen 144

Dateien mit 7-Zip verschlüsseln	144
Cloud-Speicher mit Boxcryptor sicher nutzen	147

7. Datenschutzeinstellungen per Programm 153

Datenschutz-Tools: Vor- und Nachteile	153
O&O ShutUp10 installieren	154
Einzelne Einstellungen individuell vornehmen	154
Automatisch optimaler Datenschutz	155
Werkseinstellungen – zurück auf Anfang	157

Stichwortverzeichnis 158

Windows-Datenschutz-Checkliste

Ein Windows-PC ist kein Flugzeug, bei dem kleine Fehler über Leben oder Tod entscheiden können. Trotzdem können falsche Einstellungen oder riskante Aktionen auch hier tief greifende Folgen für Datenschutz und Datensicherheit haben. Deshalb stelle ich an den Anfang dieses Buches eine Datenschutz-Checkliste. Sie fasst kompakt zusammen, was es in den verschiedenen Bereichen besonders zu beachten gilt, und verweist für ausführlichere Beschreibungen auf die entsprechenden Seiten im Buch.

So können Sie den Istzustand analysieren und schnell erkennen, wo Handlungsbedarf besteht. Außerdem können Sie diese Liste auch später immer mal wieder schnell durchgehen, um sich zu vergewissern, dass Sie immer noch ausreichend geschützt sind. Denn die Datenschutzeinstellungen von Windows haben die unangenehme Eigenschaft, beispielsweise durch Funktions-Updates gern mal verändert bzw. auf ihre eher »gesprächigen« Standardeinstellungen zurückgesetzt zu werden.

- Verwenden Sie ein lokales Benutzerkonto? _____ ⇒ Seite 8
- Welche Daten hat Microsoft über Sie gespeichert? _____ ⇒ Seite 23
- Synchronisiert Ihr Konto unnötige Daten? _____ ⇒ Seite 29
- Ist das Windows-Insider-Programm deaktiviert? _____ ⇒ Seite 31
- Sind die Windows-Datenschutz-Optionen optimal? _____ ⇒ Seite 34
- Ist der App-Zugriff auf Hardware und Daten beschränkt? _____ ⇒ Seite 46
- Verrät der Sperrbildschirm ungewollt vertrauliche Daten? _____ ⇒ Seite 84
- Sucht die lokale Dateisuche auch wirklich nur lokal? _____ ⇒ Seite 88
- Sind die Cloud-Funktionen der Windows-Sicherheit aus? _____ ⇒ Seite 90
- Ist der Cloud-Verlauf der Zwischenablage deaktiviert? _____ ⇒ Seite 93

- Ist Cortana gründlich deaktiviert? _____ ⇒ Seite 95
- Sind die Datenschutzlücken der Skype-App dicht? _____ ⇒ Seite 101
- Sind die Edge-Einstellungen für Datenschutz optimal? _____ ⇒ Seite 104
- Wird unerwünschtes Tracking beim Surfen blockiert? _____ ⇒ Seite 118
- Gibt es Benutzerprofile für sensible Webaktionen? _____ ⇒ Seite 123
- Ist der Application Guard für Edge eingerichtet? _____ ⇒ Seite 125
- Sind zusätzliche Tracking-Blocker in Edge installiert? _____ ⇒ Seite 127
- Ist die Erweiterung HTTPS Everywhere aktiv? _____ ⇒ Seite 138
- Löscht Edge Browserdaten beim Beenden automatisch? _____ ⇒ Seite 142
- Ist 7-Zip zum Verschlüsseln von Daten installiert? _____ ⇒ Seite 144
- Ist Boxcryptor für sicheren Cloud-Speicher eingerichtet? _____ ⇒ Seite 147

Freihand- und Eingabeerkennung verbessern

Windows-Einstellungen: *Datenschutz/Diagnose und Feedback*

Ist diese Option eingeschaltet, übermittelt Windows alle Ihre Eingaben in die Cloud, damit Microsoft seine Funktionen für Vorschläge und Korrekturen weiterentwickeln kann.

Hinweis: Wenn Sie die darüber stehende Option *Diagnosedaten* auf *Standard* setzen, wird das Verbessern der Freihand- und Eingabeerkennung automatisch deaktiviert und diese Option kann dann auch nicht verändert werden.

Standard: *Ein* – Empfehlung: *Aus*

Individuelle Benutzererfahrung

Windows-Einstellungen: *Datenschutz/Diagnose und Feedback*

Ist diese Einstellung eingeschaltet, verspricht Microsoft, individueller an den Benutzer angepasste Tipps und Hinweise zu geben. Es werden deswegen keine zusätzlichen Daten erhoben, nur die ohnehin ermittelten Daten noch intensiver ausgewertet. Insofern kann man sich überlegen, ob man an solchen individuellen Empfehlungen interessiert ist.

Standard: *Ein* – Empfehlung: *Aus*

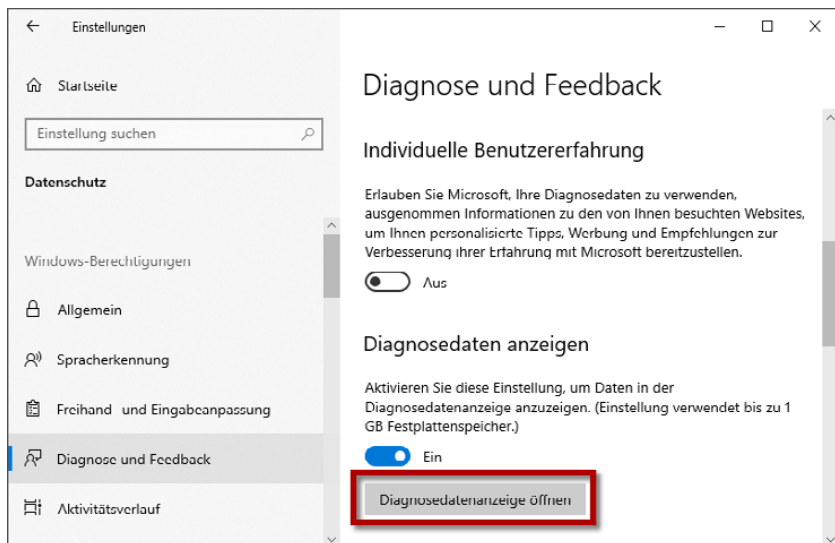
Diagnosedaten anzeigen

Windows-Einstellungen: *Datenschutz/Diagnose und Feedback*

Um die neue Diagnosedatenanzeige (siehe Seite 26) nutzen zu können, muss diese Einstellung zumindest vorübergehend aktiviert werden. Auf Dauer sollte sie aber abgeschaltet bleiben, um den Speicherplatz der Diagnosedaten freizugeben.

Beachten Sie dazu auch die Schaltfläche darunter, mit der Sie jederzeit Ihre *Diagnosedatenanzeige öffnen* können.

Standard: *Ein* – Empfehlung: nur bei Bedarf einschalten



Diagnosedaten löschen

Windows-Einstellungen: *Datenschutz/Diagnose und Feedback*

In diesem Abschnitt finden Sie eine *Löschen*-Schaltfläche, mit der Sie alle Diagnosedaten, die Microsoft in seinen Systemen zu diesem Gerät gesammelt hat, löschen lassen können.

Empfehlung: bei aktiver Diagnose regelmäßig nutzen



Feedbackhäufigkeit

Windows-Einstellungen: *Datenschutz/Diagnose und Feedback*



Gern fragt Windows den Anwender nach seiner Meinung zu bestimmten Aspekten wie beispielsweise neuen Funktionen oder dem Auftreten bestimmter Probleme. Die Antworten werden selbstverständlich an Microsoft übermittelt und ausgewertet. Allerdings kann man solche Fragen einfach ignorieren. Dann ist es aber sinnvoller, sie von vornherein ganz zu unterbinden, indem man hier die Einstellung *Nie* wählt.

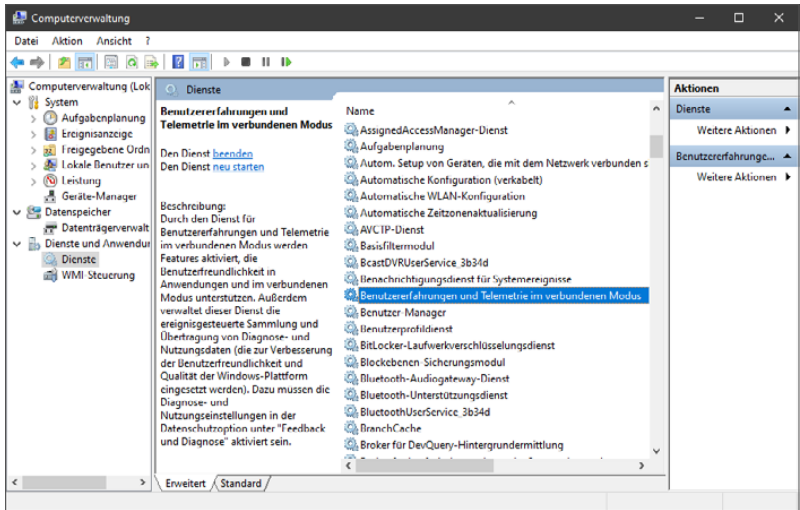
Standard: *Automatisch* – Empfehlung: *Nie*

Das Übertragen von Telemetrie ganz blockieren

Obwohl Microsoft bei einzelnen Windows-Editionen wie etwa Enterprise oder Student eine weitere Feedback-Stufe mit noch weniger Daten erlaubt, stellt sich der Softwareriese nicht ganz uneigennützig auf den Standpunkt, dass es ganz ohne Diagnosedaten nun mal nicht gehe.

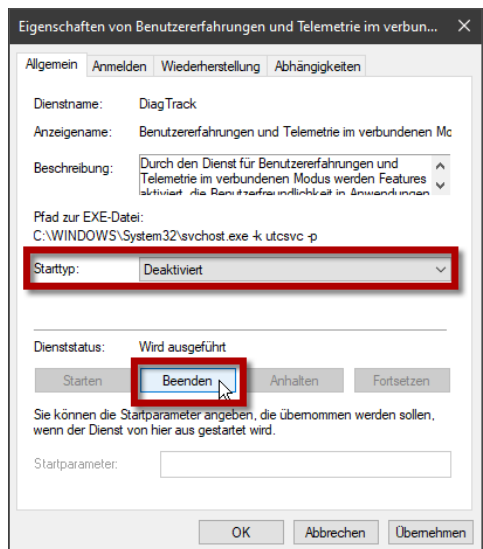
Dass das so nicht ganz stimmt, zeigt eine Untersuchung des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Die haben das Erheben und Übermitteln von Diagnosedaten bei Windows 10 näher unter die Lupe genommen und dabei einen Windows-Dienst als zuständige Instanz für das Übermitteln der Daten an Microsoft ausgemacht. Tests haben gezeigt, dass man diesen Dienst deaktivieren kann, ohne Nachteile befürchten zu müssen. Es wirkt sich beispielsweise nicht nachteilig auf den Empfang von Windows-Updates oder das Nutzen anderer Windows-Dienste aus.

- 1 Klicken Sie mit der rechten Maustaste auf das Windows-Symbol der Taskleiste (oder drücken Sie +).
- 2 Wählen Sie im Menü den Punkt *Computerverwaltung*.
- 3 Öffnen Sie in der Navigationsleiste am linken Rand *Dienste und Anwendungen/Dienste*.
- 4 Suchen Sie in der Liste der Dienste den Eintrag *Benutzererfahrung und Telemetrie im verbundenen Modus* und doppelklicken Sie darauf.



- 5 Klicken Sie im anschließenden Dialog auf *Beenden*, um den Dienst zu deaktivieren.
- 6 Wichtig: Wählen Sie außerdem bei *Starttyp* die Option *Deaktiviert*, damit Windows den Dienst nicht wieder eigenmächtig reaktivieren kann.

Wichtig: Durch die halbjährlichen Funktions-Updates werden diese Einstellungen leider immer wieder rückgängig gemacht. Deshalb müssen sie nach jedem Funktions-Update erneut wie hier beschrieben vorgenommen werden.



Warnhinweis

Das Deaktivieren dieses Dienstes ist nach derzeitigem Kenntnisstand unproblematisch. Allerdings ist nicht auszuschließen, dass sich in Einzelfällen doch Probleme ergeben können oder dass Microsoft darauf reagiert, wenn immer mehr Benutzer diese Methode anwenden. Im Fall von Problemen lässt sich der Dienst aber ebenso schnell wieder reaktivieren.

Aktivitätsverlauf

Mit dem Funktions-Update von April 2018 führte Microsoft den geräteübergreifenden Aktivitätsverlauf (Timeline) für Windows ein. Dieser ist aus Sicht des Datenschutzes nicht unproblematisch. Wenn sich mehrere Personen einen PC (und das Benutzerkonto) teilen, kann einer sofort sehen, was der andere gemacht hat. Dies lässt sich vermeiden, indem jeder Anwender sein eigenes Benutzerkonto verwendet.

Einzelne Einträge aus dem Aktivitätsverlauf löschen

Eventuell möchten Sie den Aktivitätsverlauf prinzipiell nutzen und nur gelegentlich einzelne Einträge löschen, damit diese nicht übermittelt oder von anderen gesehen werden können? Wenn Sie einen Eintrag im Aktivitätsverlauf mit der rechten Maustaste anklicken, finden Sie im Kontextmenü den Befehl *Entfernen*, der den jeweiligen Eintrag löscht. Alternativ können Sie mit *Alle von "..."* *löschen* auch gleich alle Einträge des jeweiligen Tages aus dem Aktivitätsverlauf entfernen.



Komplizierter wird es, wenn man auf mehreren Geräten die Synchronisierung des Aktivitätsverlaufs nutzt. Diese ermöglicht es beispielsweise, eine unterwegs am Notebook begonnene Tätigkeit später zu Hause am PC einfach fort-

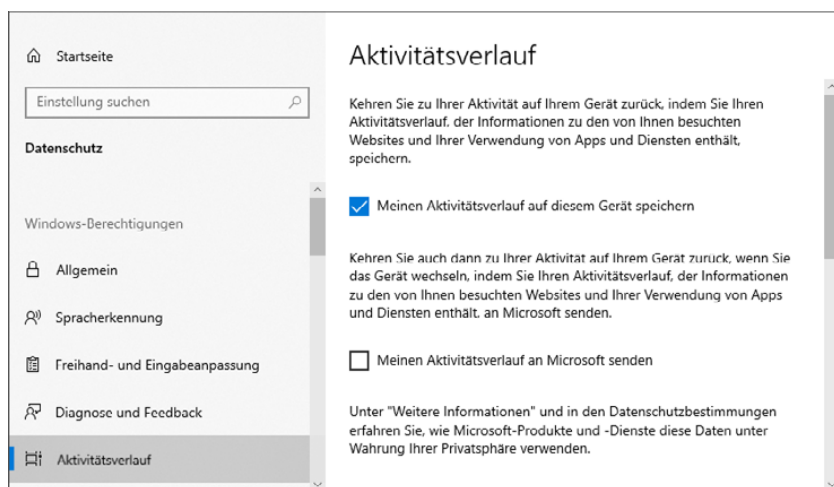
zusetzen. Allerdings erfolgt das Synchronisieren über das Microsoft-Konto und die Cloud, und auch hier besteht bei geteiltem Konto die Möglichkeit, dass die Anwender sich gegenseitig kontrollieren können. In den *Einstellungen* unter *Datenschutz/Aktivitätsverlauf* können Sie aber festlegen, ob und wie synchronisiert werden soll.

Meinen Aktivitätsverlauf auf diesem Gerät speichern

Windows-Einstellungen: *Datenschutz/Aktivitätsverlauf*

Diese Einstellung steuert, ob Aktivitäten, die Sie auf diesem Gerät ausüben, in den Aktivitätsverlauf aufgenommen werden sollen. Sie können den Aktivitätsverlauf unabhängig davon nutzen. Aber wenn Sie diese Option ausschalten, werden in der Timeline nur Aktivitäten anderer Geräte angezeigt.

Standard: *Ein* – Empfehlung: Keine



Meinen Aktivitätsverlauf an Microsoft senden

Windows-Einstellungen: *Datenschutz/Aktivitätsverlauf*

Diese Einstellung legt fest, ob die Aktivitäten, die Sie auf diesem PC ausüben, per Cloud mit Ihren anderen Geräten synchronisiert werden sollen. Sie kön-

nen den Aktivitätsverlauf unabhängig davon nutzen, aber wenn diese Option ausgeschaltet ist, werden Aktivitäten von diesem PC auf anderen Geräten nicht angezeigt.

Standard: *Ein* – Empfehlung: Keine

Position

Windows kann aus verschiedenen Quellen Informationen über den aktuellen Standort Ihres PCs beziehen. Selbst wenn kein GPS-Empfänger verbaut ist, können Informationen über verfügbare WLANs (teilweise recht genau), Mobilfunkmasten oder Daten der Internetwahl und verwendete IP-Adressen (eher ungenau) eine Ortsbestimmung ermöglichen.

Diese Angaben werden für ortsbezogene Dienste genutzt, aber auch zur Auswertung an Microsoft oder die Entwickler einzelner Apps übermittelt. Die relevanten Optionen hierzu finden Sie in den *Einstellungen* in der Rubrik *Datenschutz/Position*.

Zugriff auf den Standort auf diesem Gerät zulassen

Windows-Einstellungen: *Datenschutz/Position*

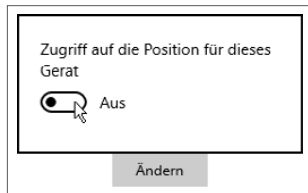
Diese Einstellung steuert sozusagen die grundlegende Funktion zur Standortermittlung. Ist sie eingeschaltet, kann Windows die Position bestimmen und dazu ggf. auf vorhandene Hardware wie einen GPS-Empfänger zugreifen. Schalten Sie diese Einstellung aus, wird die Standorterkennung deaktiviert, und weder Windows selbst noch zusätzliche Apps können auf Standortdaten zugreifen.

Ob man das möchte, hängt von den individuellen Ansprüchen ab. Ist man mit einem Notebook oder Tablet unterwegs und möchte standortbasierte Dienste nutzen oder sich navigieren lassen, muss diese Option eingeschaltet sein. Auf einem stationären PC hingegen wird man solche Funktionen eher weniger benötigen.

Hinweis: Diese Einstellung wird etwas anders als die meisten Datenschutzeinstellungen verwendet, da Sie hier zunächst auf die *Ändern*-Schaltfläche

klicken müssen und dann erst im eingeblenden Einstellungsdialog die eigentliche Wahl zwischen *Ein* oder *Aus* vornehmen.

Standard: *Ein* – Empfehlung: Keine



Zulassen, dass Apps auf Ihren Standort zugreifen

Windows-Einstellungen: *Datenschutz/Position*

Diese Option steuert, ob Apps auf die Standortdaten zugreifen dürfen. Ist sie eingeschaltet, können Sie weiter unten in der Liste der Apps festlegen, welchen davon dies erlaubt sein soll und welchen nicht. Diese Option lässt sich nur einschalten, wenn die Standorterkennung für den PC insgesamt mit der darüber stehenden Einstellung aktiviert ist.

Beachten Sie hierzu den Hinweis, dass eine Beschränkung des Zugriffs nur für Apps aus dem Microsoft Store gilt. Klassische Desktop-Anwendungen können auf diese Weise nicht eingeschränkt werden (wohl aber durch das Deaktivieren der Standortermittlung insgesamt).

Standard: *Ein* – Empfehlung: Keine