Windows 10 Datenschutz

SCHLUSS MIT DEM DATENSAMMELN!

Mit den Standardeinstellungen von Windows 10 gibt man als Nutzer zahlreiche Daten für Microsoft und sogar Dritte Preis. Wir erklären, wie sich Microsofts Sammelwut eindämmen lässt. Von Jan Purrucker

Windows 10 erfreut sich durch Neuerungen wie den Verzicht auf die Kacheloberfläche, der Rückkehr des Startmenüs und Microsofts kostenloser Upgradepolitik deutlich größerer Beliebtheit als Windows 8. Laut Microsoft wurde das neue Betriebssystem bereits innerhalb der ersten 24 Stunden nach dem Start über 14 Millionen Mal installiert (bei Windows 8 waren es vier Millionen verkaufte Exemplare in vier Tagen). Allerdings werden Windows 10 und Microsoft von Datenschützern auch für die im Vergleich zu den Vorgängern augenscheinlich größere Menge an abgefragten Nutzerdaten kritisiert.

Im Netz finden sich zahlreiche Meldungen und teils lautstarke Kritik zur Vergabe von individuellen Werbe-IDs, Zwangsupdates, dem Abfragen von Standort und Schreibverhalten sowie der angeblichen Weitergabe von WLAN-Passwörtern. Auch Microsofts neue digitale Assistentin und Siri-Konkurrentin Cortana wird kritisiert, schließlich greift sie (und somit auch Microsoft) unter anderem auf Informationen aus dem Kalender und aus dem Inhalt von E-Mails und SMS zu.

Zwar lässt sich die Weitergabe von Daten durch das Abschalten der entsprechenden Optionen in vielen Fällen bereits bei der Installation von Windows 10 beziehungsweise bei dem Upgradevorgang einschränken, allerdings müssen Sie dafür statt auf den großen Button für die Expresseinstellungen auf die deutlich kleinere Schaltfläche »Einstellungen anpassen« klicken, die Sie dann zu den Datenschutzoptionen führt.

Die Einstellungen können Sie auch nach der Installation von Windows 10 noch verändern, jedoch verstecken sich die Optionen teils in unterschiedlichen und unübersichtlichen Menüs. Zudem wird bei vielen Optionen erst beim Durchforsten der extrem umfangreichen Geschäftsbedingungen halbwegs klar, welche Daten an wen und unter welchen Umständen gesammelt und weitergegeben werden – wenn überhaupt.

In diesem Guide zeigen wir Ihnen deshalb, wo Sie die verschiedenen Datenschutzoptionen von Windows 10 finden und wie Sie die Menge an mit Microsoft und Werbepartnern geteilten Informationen reduzieren können. Während sich die Einstellungen zur Privatsphäre in Windows 8.1 auf fünf Kategorien (»Allgemein«, »Position«, »Webcam«, »Mikrofon« und »Weitere Geräte«) aufteilen, wächst diese Anzahl bei Windows 10 auf zwölf. Sie finden die Optionen, indem Sie auf das Infocenter-Symbol auf der rechten Seite der Taskleiste klicken und anschließend »Alle Einstellungen« wählen.

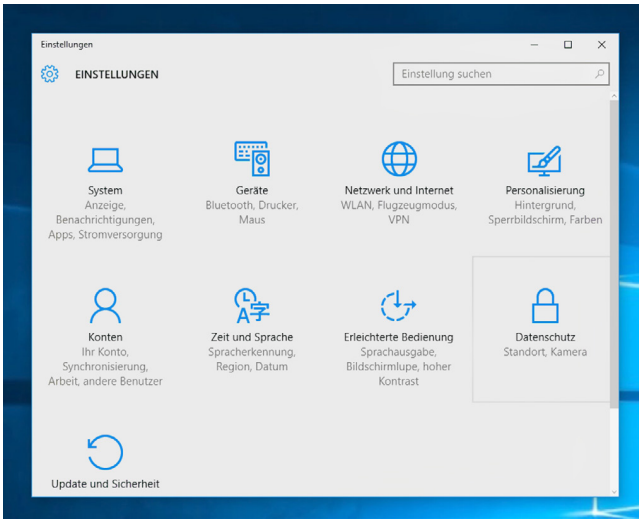
Datenschutz und allgemeine Einstellungen

Unter »Allgemein« haben Sie die Möglichkeit, Apps die Verwendung der Werbe-ID zu verbieten, um so das Erstellen und Anzeigen von auf Sie zugeschnittener Werbung (durch Dritte) zu verhindern. Lassen Sie diese und die zugehörigen Optionen aktiviert, generiert Microsoft eine Werbe-ID, die Auskunft über ihre Favoriten, das Schreibverhalten, den Browserverlauf, installierte Programme, Alter, Geschlecht und andere persönliche Informationen enthält. Neben personalisierter Werbung soll die ID auch die Nutzung von unterschiedlichen Microsoft-Geräten (Xbox One, Windows Phone, Cloud-Dienste) verbessern.

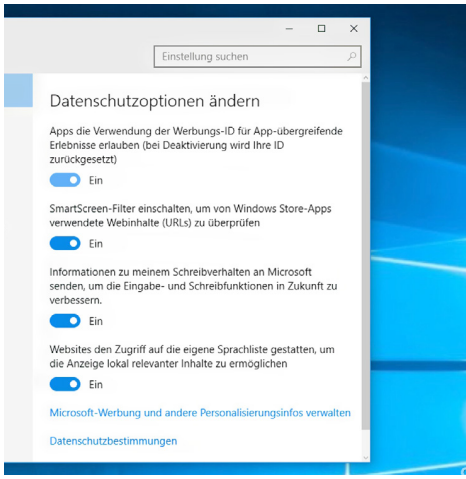
Kennenlernen beenden

Die Einstellungen zu Position, Kamera und Mikrofon sind bereits aus Windows 8 bekannt, allerdings können Sie die Optionen jetzt teils deutlich individueller einstellen.

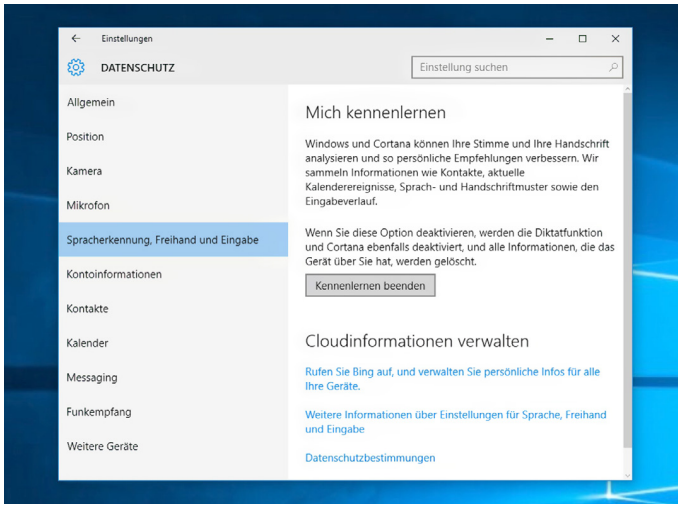
Ein Klick auf das an eine Sprechblase erinnernde Symbol in der Taskleiste öffnet das Infocenter. Hier wählen Sie den Punkt »Alle Einstellungen«.



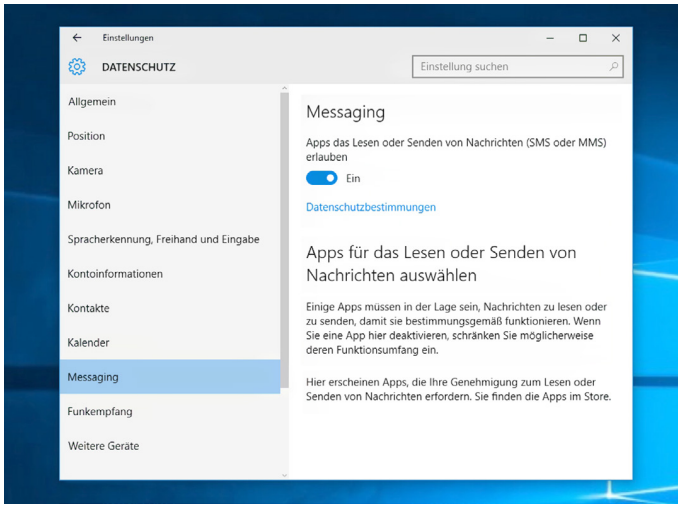
In der Übersicht finden Sie die Menüs sowohl für den Datenschutz als auch für Netzwerk, Internet (WLAN), Update und Sicherheit.



Die meisten und wichtigsten Datenschutzoptionen lassen sich im entsprechenden Menüpunkt anpassen und deaktivieren.



Cortana macht Siri Konkurrenz und will dafür ähnlich viel von ihrem Nutzer wissen. Allerdings lässt sich die Option leicht abschalten.



Manche der Datenschutzoptionen sind klar auf mobile Geräte (SMS, MMS) ausgelegt, aber trotzdem auf Desktop-PCs vorhanden.

So lässt sich der Zugriff auf die entsprechenden Daten und die Nutzung von Webcam und Mikrofon nicht mehr nur komplett de- oder aktivieren, sondern auch nur für einzelne Anwendungen anpassen.

Eine weitere Neuerung ist, dass Windows 10 seine Nutzer jetzt offiziell »kennenlernen will«. Dafür sammeln Windows und Cortana Daten zu »Spracherkennung, Freihand und Eingabe«, also Ihrer Stimme, Ihrer Handschrift (Tablets) und Ihrem Schreibverhalten. Auch Informationen zu Kontakten und Kalendereinträgen gehören dazu. Microsoft speichert alle Daten in der Cloud, um sie beim Einloggen mit dem Microsoft-Account auch auf anderen Computern des Nutzers zur Verfügung zu stellen.

Dieser Punkt gehört somit zu den umfangreichsten Sammeloptionen, und wenn Ihnen die gute Cortana nicht zu sehr ans Herz gewachsen ist, sollten Sie die Assistentin deaktivieren beziehungsweise die gespeicherten Informationen durch den Klick auf »Kennenlernen beenden« löschen. Daneben können Sie über den darunter stehenden Link noch die in Bing gespeicherten Daten zu Suchanfragen entfernen.

Geteilte Passwörter?

Die WLAN-Einstellungen haben bereits im Vorfeld der Veröffentlichung von Windows 10 für viel Wirbel gesorgt, weil Microsoft angeblich ungefragt WLAN-Passwörter mit Freunden teilt, was von mobilen Windows-Geräten unter dem Namen »Wi-Fi Sense« bekannt ist. Das entspricht allerdings nicht den Tatsachen, auch wenn es die Funktion unter der Bezeichnung »WLAN-Optimierung« tatsächlich in Windows 10 gibt.

Teil der WLAN-Optimierung ist die Einstellung »Ausgewählte Netzwerke freigeben für ...«, die Sie unter »Einstellungen/Netzwerk und Internet/WLAN/WLAN-Einstellungen verwalten« finden. Die drei auswählbaren Kontaktarten sind Outlook.com, Skype und Facebook. Allerdings müssen Sie selbst dann, wenn Sie die Freigabe für eine der Kontaktarten per Häkchen aktivieren, anschließend immer noch die gewünschten Netzwerke manuell für die Funktion freischalten – und das ist auch nur nach einer erneuten Eingabe des WLAN-Passworts möglich. Ohne Ihr eigenes Zutun teilt Microsoft also keinerlei WLAN-Passwörter mit Ihren Kontakten.

Bei den Einstellungen zu Kontoinformationen, Kontakten, Kalender und Messaging können Sie wieder wählen, welche Apps auf die Daten zugreifen dürfen, oder Sie schalten die Funktionen ganz ab. Im Reiter »Weitere Geräte« lässt sich festlegen, ob und welche Apps Informationen mit Geräten austauschen dürfen, die im gleichen WLAN-Netz sind. Außerdem kann Anwendungen hier die Nutzung bestimmter Geräte erlaubt werden, um so beispielsweise den Zugriff auf den USB-Speicher zu erleichtern.

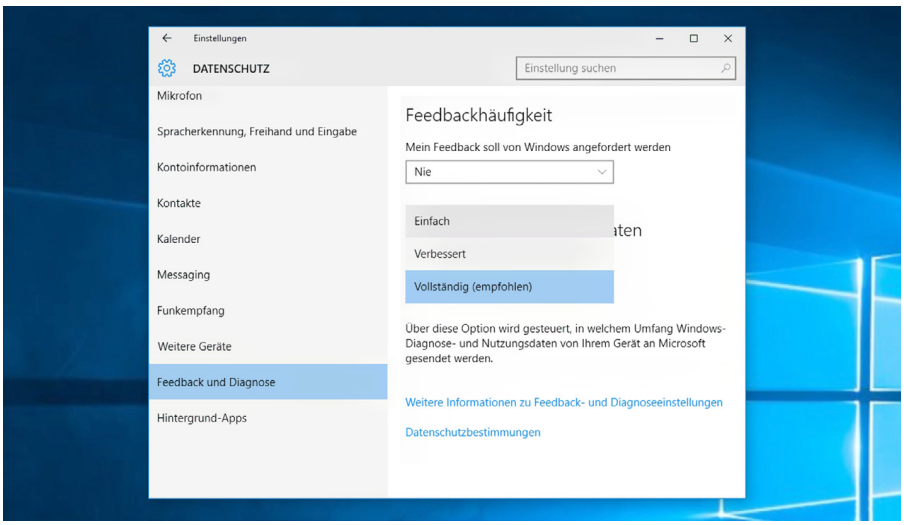
Automatische Updates

Mit Windows 10 lassen sich die automatischen Updates zwar nicht mehr komplett deaktivieren, aber Sie können den Vorgang über »Update und Sicherheit/Windows Update/Erweiterte Optionen« zumindest so einstellen, dass sie notwendige Neustarts selbst planen. Nutzer von Windows 10 Pro können außerdem die Updates zurückstellen und so das Herunterladen und Installieren von Updates um einige Monate verzögern.

Gerade wenn Sie kein zusätzliches Virenschutzprogramm nutzen, lohnt sich zudem ein Blick in den Windows Defender. Hier können Sie festlegen, ob Windows 10 etwa Daten über gefundene Schadsoftware an Microsoft übermitteln darf.

Zugriff auf private Inhalte

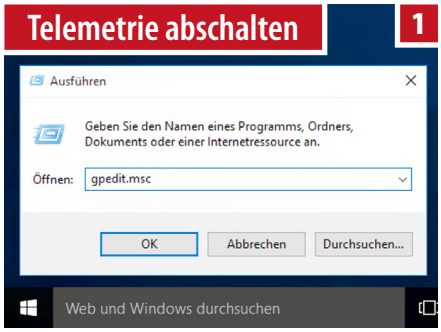
Um zu verhindern, dass Microsoft regelmäßig Ihre Meinung zu Windows wissen will, können Sie die »Feedbackhäufigkeit« im Reiter »Feedback und Diagnose« auf »Nie« stellen. Wesentlich interessanter ist allerdings der Bereich »Diagnose- und Nutzungsdaten«, in dem Sie steuern können, wie oft und in welchem Umfang das Betriebssystem solche Daten an Microsoft sendet. Sofern Sie keine Enterprise-Version von Windows 10 nutzen, lässt sich das Versenden dieser Daten allerdings nur auf »Einfach« stellen. Offiziell können Sie die Telemetrie als Nutzer von Windows 10 Home oder Pro also nicht vollständig deaktivieren.



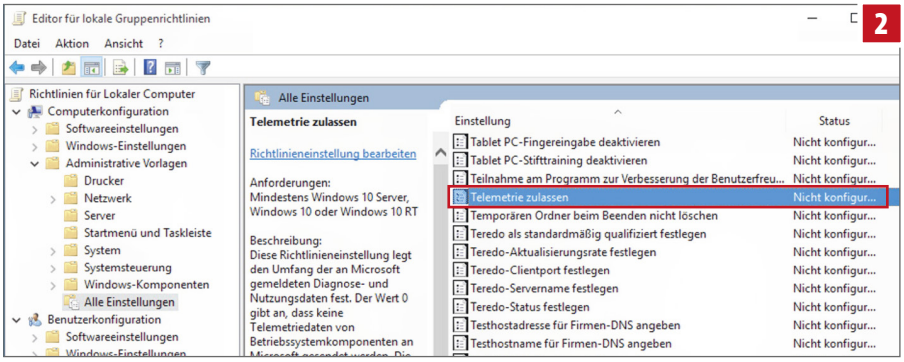
Während Sie diese Feedback-Aufforderung einfach deaktivieren können, lässt sich die Telemetrie, also das Übermitteln von persönlichen Daten, nur über Umwege verhindern.

Die klassische Aufteilung in verschiedene Versionen (7, 8, 8.1) gehört demnach der Vergangenheit an.

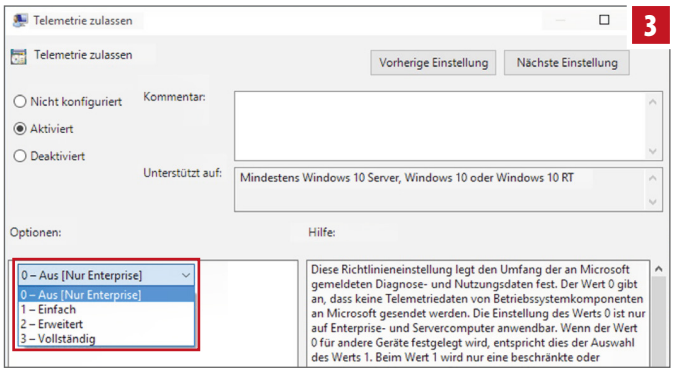
Telemetrie abschalten



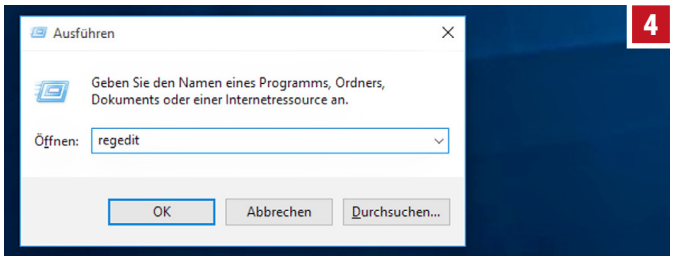
Über Win + R rufen Sie die Ausführen-Maske auf und tippen den »gpedit.msc« ein.



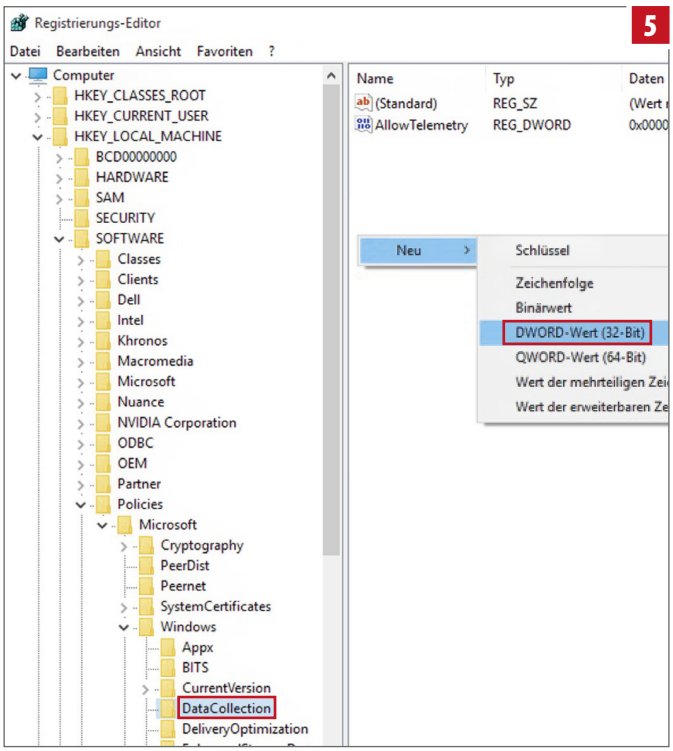
Im Editor für lokale Gruppenrichtlinien finden Sie den Punkt »Telemetrie zulassen«.



Hier können Nutzer von Windows 10 Enterprise die Telemetrie abschalten. Home und Pro senden zwar weiterhin, legen aber die für Schritt 3 notwendige Datei an.



Kommt es bei Schritt 1 zu einer Fehlermeldung, öffnen sie über »regedit« den Registrierungseditor.



Hier versteckt sich der Punkt »DataCollection«. Sofern noch nicht vorhanden, legen Sie über einen Rechtsklick einen neuen DWORD-Wert an.

Schnüffeltelemetrie abschalten

Nutzer von Windows 10 Home und Pro können über Umwege die Telemetrieoptionen ausschalten und die entsprechenden Dienste und Anwendungen sperren – allerdings geschieht das dann ohne Garantie und auf eigenes Risiko. Schließlich kann Microsoft Windows 10 durch Updates ständig anpassen und so eventuelle Lücken schnell schließen. So konnte man etwa in der Vergangenheit Windows das Versenden von Daten noch durch Anpassen der Host-Datei manuell verbieten. Mittlerweile ist das in Windows 10 nicht mehr möglich. Dennoch können Sie es Windows etwas schwerer machen, ihre Daten an Microsoft weiterzugeben.

Schritt 1: Sie können entweder auf ein Open-Source-Tool wie DisableWinTracking oder DoNotSpy10 zurückgreifen oder die Einstellungen selbst vornehmen. Hierfür öffnen Sie zuerst »Ausführen« (Win + R) und tippen »gpedit.msc« ein. Mit einem Druck auf die Enter-Taste sollte sich der Editor für lokale Gruppenrichtlinien öffnen (sollte eine Fehlermeldung erscheinen, gehen Sie einfach direkt zum nächsten Schritt). Hier findet sich unter »Computerkonfiguration/Administrative Vorlagen/Alle Einstellungen« die Option »Telemetrie zulassen«. Nach einem Doppelklick darauf aktivieren sie den Dienst und wählen bei den Optionen »0-Aus«. Auf Enterprise-Systemen ist die Telemetrie jetzt deaktiviert, Home- und Pro-Versionen von Windows 10 übernehmen zwar die Einstellung, allerdings werden dennoch weiterhin Daten geschickt – der Schritt ist trotzdem vonnöten.

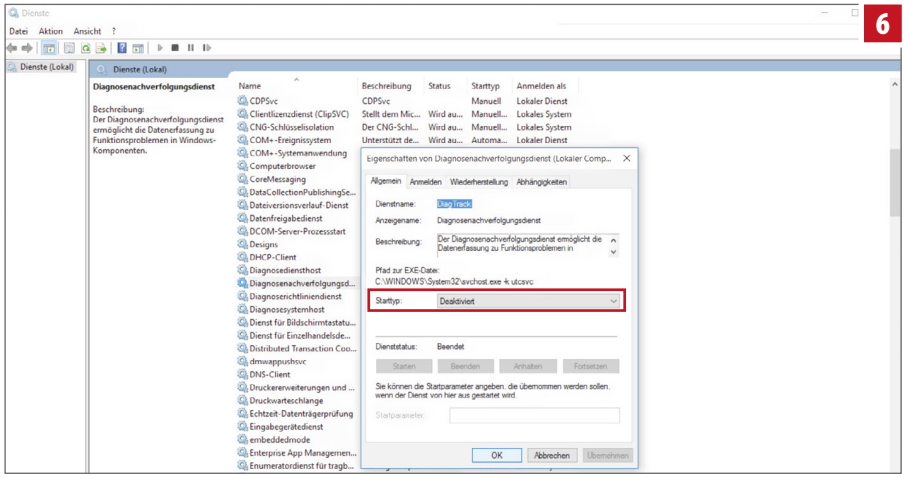
Schritt 2: Dieser Schritt ist nur notwendig, wenn bei Schritt 1 eine Fehlermeldung erscheint, Sie also nicht auf den Editor für lokale Gruppenrichtlinien zugreifen können. Über »Ausführen« und den Befehl »regedit« öffnet sich der »Registrierungs-Editor«. Navigieren Sie hier zu »HKEY_LOCAL_MACHINE/SOFTWARE/Policies/Microsoft/Windows/DataCollection«. Dort legen Sie über einen Rechtsklick einen neuen DWORD-Wert (32 Bit) an und benennen ihn »AllowTelemetry« (Wert 0 sollte standardmäßig ausgewählt sein).

Schritt 3: Zum Schluss müssen Sie noch die entsprechenden Dienste zum Versenden von Daten deaktivieren. Dafür klicken Sie mit der rechten Maustaste auf das Windows-Logo und wählen »Computerverwaltung« aus. Dort finden sie die Dienste »Diagnosenachverfolgungsdienst« und »dmwappushsvc«. Nachdem Sie beide Dienste deaktiviert und beim Starttyp »Deaktiviert« ausgewählt haben, sollte die Datenübertragung von Windows 10 an Microsoft deaktiviert sein.

Wie erwähnt, geschieht das jedoch ohne Garantie und auf eigenes Risiko – möglicherweise treten vereinzelt ungewollte Konsequenzen auf, uns sind aber (noch) keine bekannt.

Kryptische Datenschutzbestimmungen

Laut den Datenschutz- und Lizenzbestimmungen von Microsoft, die insgesamt über 110.000 Zeichen umfassen, speichert der Konzern personenbezogene Daten und behält sich das Recht vor, sogar den



In der Computerverwaltung finden Sie die Dienste »Diagnosenachverfolgungsdienst« und »dmwappushsvc«. Beenden Sie beide Dienste und deaktivieren Sie deren automatischen Start.

Inhalt von E-Mails und Ordnern auf der Festplatte weiterzugeben, etwa wenn diese beim Verdacht einer Straftat des Nutzers durch eine Behörde angefordert werden. Auch zum Schutz der Windows-Nutzer vor Spam und Hackern werden Daten gespeichert. Diese und ähnliche Punkte sind teilweise absichtlich recht schwammig formuliert. Laut Gesetz gibt es bei der Erhebung von Daten nämlich eine Zweckbindung. Informationen, die zum Beispiel ursprünglich für das Ausliefern von Updates erhoben wurden, dürfen später nicht für Werbeprofile verwendet werden. Daher listet Microsoft in seinen Datenschutzbestimmungen zahlreiche Verwendungszwecke auf und sichert sich so vermeintlich ab – ob und was davon nach europäischem Recht Bestand hat, steht aber auf einem anderen Blatt.

Viel Beachtung fand auch ein Absatz, indem Microsoft sich vorbehält, geistiges Eigentum zu schützen und gegen Raubkopierer vorzugehen. Allerdings kam es hier nicht zuletzt wegen der häufig ans Unverständliche grenzenden deutschen Übersetzung zu Missverständnissen. Der Konzern weist damit lediglich darauf hin, dass Software, die nur über Umwege installiert oder gestartet (Cracks) werden kann, nach einem Windows-Update möglicherweise nicht mehr richtig funktioniert.

Generell lässt sich sagen, dass die Datenschutzbestimmungen von Windows 10 nicht nur für Laien alles andere als verständlich formuliert sind und es an vielen Stellen auch zu Konflikten zwischen amerikanischem und europäischem Recht kommt. Nicht zuletzt deswegen zögern viele Nutzer noch, auf Windows 10 umzusteigen. Allerdings beziehen sich die meisten Absätze der Bestimmungen nicht auf Windows 10 im Speziellen, sondern auf Windows im Allgemeinen. Es gibt zwar innerhalb der Bestimmungen unter dem Punkt »Dienstspezifische Details« einen eigenen Bereich zu Windows, der damit explizit Windows 10 meint, die viel diskutierte Passage zu der Nutzung personenbezogener Daten ist aber weit davor in den allgemeinen Anmerkungen untergebracht.

Es ist also nicht immer ganz einfach, die umfangreichen Datenschutzbestimmungen richtig zu interpretieren. Aber Microsoft hat ähnlich wie Apple, Facebook und Google den Wert von Nutzerdaten erkannt und legt mit Windows 10 einen noch stärkeren Fokus darauf als in früheren Versionen des Betriebssystems. Ganz unabhängig davon wäre es aber eine Illusion zu glauben, dass man unter Windows 7 oder Windows 8.1 vor ähnlichen Interessen an den eigenen Daten gefeit sei. ★