Baden-Württemberg

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ

Datenschutzeinstellungen bei Windows 10

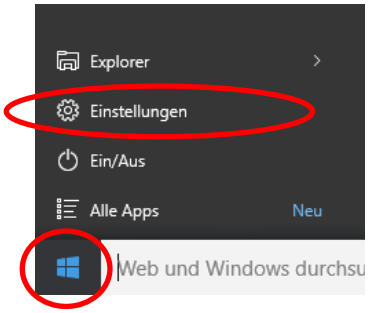
Wie Sie Windows 10 datenschutzfreundlich nutzen können

- Stand: Mai 2016 -

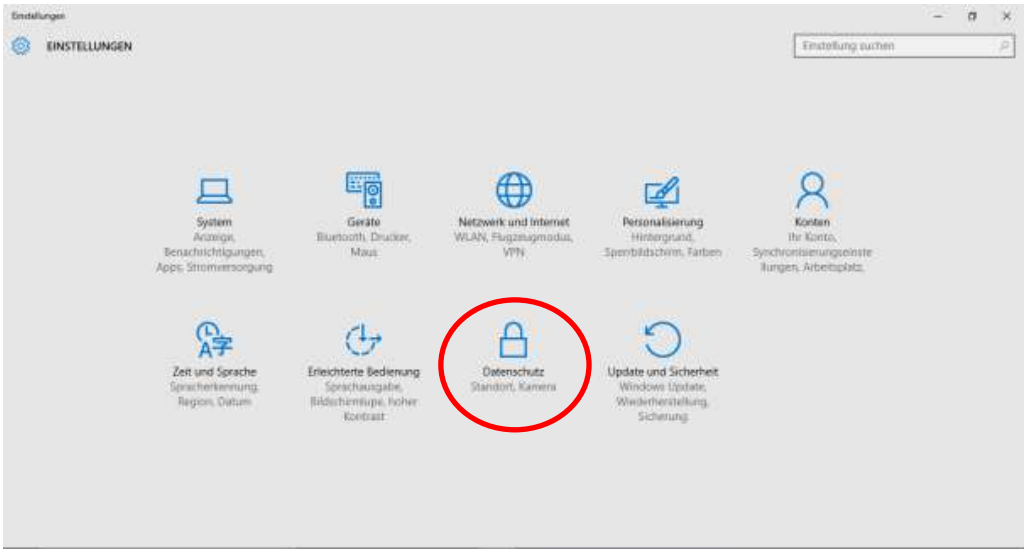
Der Landesbeauftragte für den Datenschutz in Baden-Württemberg
Königstraße 10a
70173 Stuttgart
Telefon 0711/615541-0
Telefax 0711/615541-15
E-Mail: poststelle@lfd.bwl.de
(Schutzbedürftige Daten sollten nicht unverschlüsselt per E-Mail oder via Telefax übertragen werden.)
PGP-Fingerprint: E4FA 428C B315 2248 83BB F6FB 0FC3 48A6 4A32 5962
Homepage: www.baden-wuerttemberg.datenschutz.de

Das neue Betriebssystem Windows 10 von Microsoft ist Ende Juli 2015 erschienen.[1] Besitzer von Windows 7 und 8 können ein kostenloses Upgrade auf Windows 10 erhalten. Microsoft möchte damit erreichen, dass in naher Zukunft möglichst viele Geräte mit ein und demselben Betriebssystem laufen. Windows 10 soll Microsoft auch dabei helfen, seine Cloud-Dienste – etwa Office 365 – zu etablieren. Gerade diese starke Verzahnung des neuen Betriebssystems mit der Microsoft Cloud und die Einführung eines neuen persönlichen Assistenten – genannt „Cortana“ – bringen allerdings eine Reihe von Auswirkungen in Punkto Datenschutz mit sich. Microsoft hat sich leider gegen ein aus Datenschutzsicht zu befürwortendes „Opt in“-Verfahren (Einwilligung) entschieden und setzt stattdessen auf ein „Opt out“-Konzept (Widerspruch). Dies hat zur Folge, dass Sie als Nutzer selbst aktiv werden müssen, wenn Sie nicht möchten, dass persönliche Daten über Sie gesammelt und an Microsoft übertragen werden. Wir zeigen in diesem Leitfaden, durch welche Einstellungen Sie dem Sammel-Drang nach persönlichen Daten von Microsoft entgegenhalten können.

Zunächst wechseln Sie zu den Windows 10-Einstellungen („Windows-Symbol“ -> „Einstellungen“).

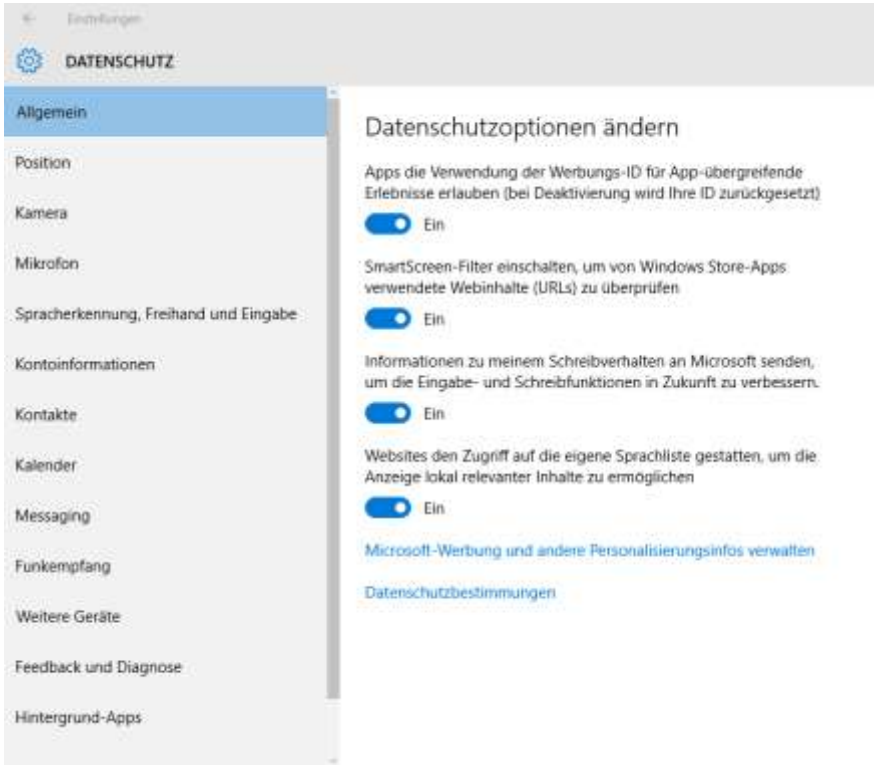


Als nächstes wählen Sie den Bereich „Datenschutz“ aus.



[1] Diese Ausführungen berücksichtigen noch nicht die Auswirkungen des Urteils des Gerichtshofs der Europäischen Union vom 6. Oktober 2015 (AZ.: C-362/14). Die europäischen Datenschutzaufsichtsbehörden stimmen derzeit noch untereinander ab, welche konkreten Folgerungen aus dem genannten Urteil für die Zulässigkeit eines Transfers personenbezogener Daten aus der Europäischen Union in die USA zu ziehen sind.

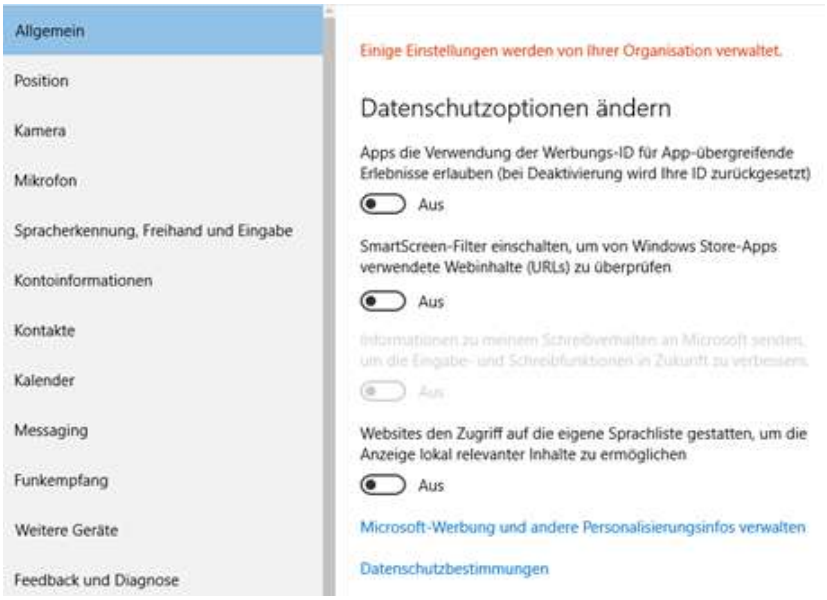
Im Bereich „Datenschutz“ lassen sich nun eine Vielzahl an Datenschutz-Einstellungen vornehmen. Die jeweiligen Einstellungen sind über die Kategorien im linken Seitenbereich zu unterschiedlichen Themen („Allgemein“, „Position“, „Kamera“, etc.) zusammengefasst:



Die meisten Optionen sind standardmäßig voreingeschaltet:

Wenn Sie eine Datenweitergabe an Microsoft unterbinden möchten, so müssen Sie die entsprechenden Optionen explizit ausschalten (Schalter auf „Aus“ stellen):

In der Kategorie „**Allgemein**“ finden sich folgende Einstellungsmöglichkeiten:



Erläuterungen zu den Datenschutzoptionen:

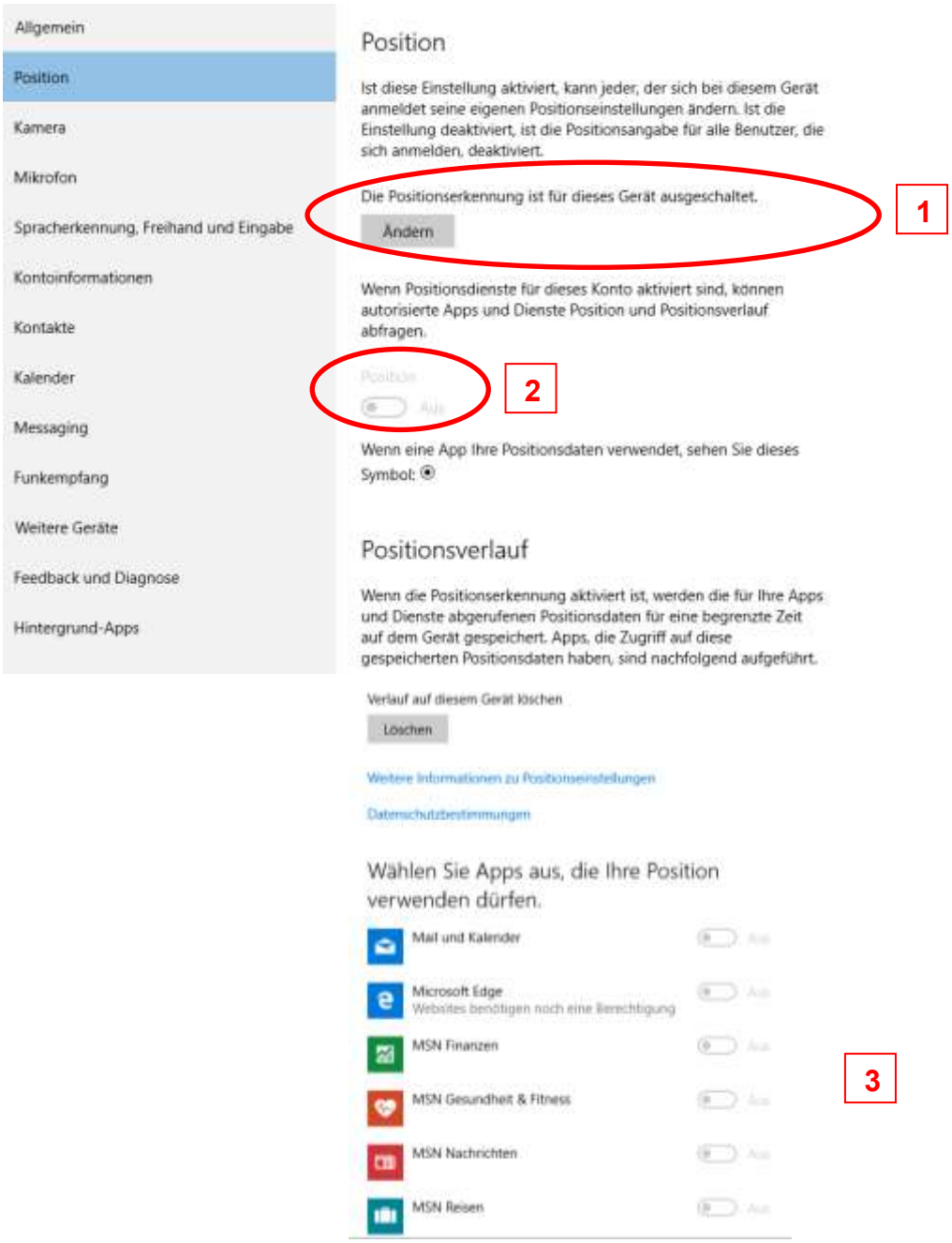
- **Werbungs-ID**: Ist diese Option eingeschaltet, so wird das Nutzungsverhalten bei unterschiedlichen Apps und Anwendungen, beim Browsen im Web, etc. analysiert und es werden in Zukunft personalisierte Werbeanzeigen angezeigt. Verwendet man unter Windows 10 ein Microsoft-Konto und nutzt dieses Microsoft-Konto auch auf anderen Geräten (Xbox, Windows Phone-Mobiltelefon, etc.), so kann die Analyse des Nutzungsverhaltens über dieses Microsoft-Konto auch geräteübergreifend erfolgen. Dies kann bedeuten, dass wenn Sie auf Ihrem PC im Internet nach einem Gebrauchtwagen suchen, Sie bei der nächsten Verwendung eines kostenlosen Spiels auf Ihrem Windows Phone-Mobiltelefon Werbung für Gebrauchtwagen angezeigt bekommen.
  Unsere Empfehlung: Schalten Sie diese Funktion aus!
- **SmartScreen-Filter:** Der SmartScreen-Filter untersucht besuchte Webseiten auf potentiell unsichere Inhalte und heruntergeladene Dateien auf Schadsoftware. Dazu wird beim Browsen im Web von jeder angefragten Webseite die Internetadresse (URL) an Microsoft zur Überprüfung gesendet. Bei heruntergeladenen Dateien werden Teile des Inhalts und zusätzliche Informationen über die Datei (bspw. Dateiname) an Microsoft gesendet. Befinden sich die angefragten URLs bzw. Dateien auf einer von Microsoft geführten schwarzen Liste mit bekannten Bedrohungen, so bekommt der Nutzer einen Warnhinweis angezeigt, der vor einem Besuch der Webseite bzw. einer Ausführung der Anwendung abrät. Laut unseren Erkenntnissen wird zudem die vollständige IP-Adresse an Microsoft übermittelt und 60 Tage lang von Microsoft gespeichert.
  Unsere Empfehlung: Schalten Sie diese Funktion aus!
  Durch die Übermittlung der IP-Adresse Ihres PCs – als personenbezogenes Datum – ist Microsoft in der Lage, ein umfangreiches Nutzungsprofil (besuchte Webseiten und installierte Anwendungen) zu bilden. Die Speicherung dieser Daten für 60 Tage erfolgt aus unserer Sicht unverhältnismäßig lange.
  Aus Sicherheitssicht mag der SmartScreen-Filter trotz der weitreichenden Datenübermittlung an Microsoft seine Berechtigung haben. Er erlaubt einen ge-

wissen Schutz vor bekannten Bedrohungen, insbesondere Schadsoftware und infizierte Webseiten können auf Ihrem Rechner enormen Schaden anrichten. Sie sollten also in jedem Fall regelmäßig Sicherheitsupdates installieren, Backups regelmäßig anfertigen und einen modernen Anti-Virenschutz einsetzen.

- **Eingabe- und Schreibverhalten:** Hier geht es vor allem um das Schreibverhalten auf einem PC mit Touchscreen bei der Verwendung eines Stifts zur Eingabe. Sendet man diese Daten an Microsoft, so kann sich dadurch die Handschrift-Erkennung verbessern. Allerdings gelangt Microsoft damit auch an alle Texte, die Sie mittels Stifteingabe schreiben.
  Unsere Empfehlung: Schalten Sie diese Funktion aus!
- **Sprachliste:** Um welche Funktionalität es sich hier genau handelt und ob dabei Daten an Microsoft übermittelt werden, geht aus den Datenschutzbestimmungen nicht hervor.
  Unsere Empfehlung: Schalten Sie diese Funktionalität aus!

Unter dem Link „Microsoft-Werbung und andere Personalisierungsinfos verwalten“ gelangt man auf eine Internetseite, unter der man unter anderem personalisierte Werbung bei der Verwendung eines Microsoft-Kontos deaktivieren kann. Unter dem Link „Datenschutzbestimmungen“ finden sich die Datenschutzbestimmungen zu Windows 10 und weiteren Microsoft-Diensten.

In der Kategorie „**Position**“ finden sich folgende Einstellungsmöglichkeiten:



Erläuterungen zu den Datenschutzoptionen:

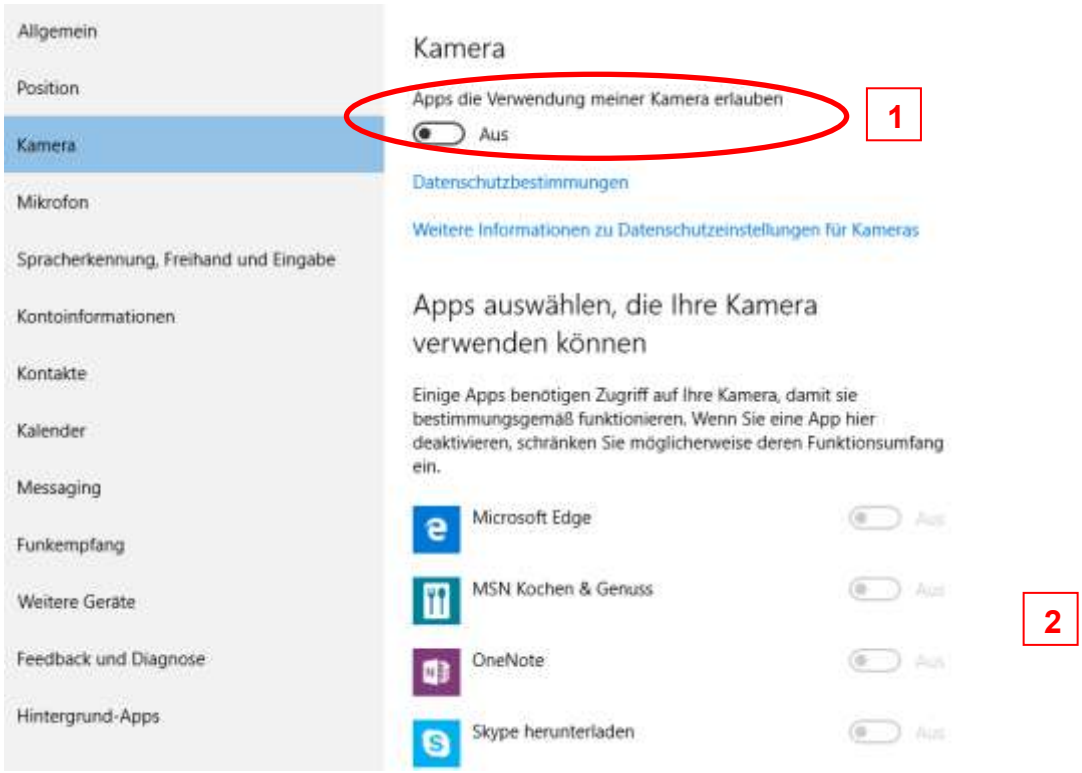
- **Positionserkennung (Einstellung Nr. 1):** Hierüber lässt sich für das Gerät festlegen, ob Positionsdaten ermittelt werden dürfen. Die Ermittlung der Positionsdaten (d.h.: Ihres Standorts) hängt von der zur Verfügung stehenden Hardware des Geräts ab. Es können die GPS-Daten, Mobilfunk- oder WLAN-Daten für die Standortermittlung herangezogen werden. Dazu werden die ermittelten Daten an Microsoft übertragen und in der von Microsoft betriebenen Standortdatenbank abgeglichen. Bei der Verwendung der Positionserkennung hilft der Nutzer Microsoft beim weiteren Ausbau der Standortdatenbank: bei jeder Anfrage werden die ermittelten Daten (insbesondere zu Mobilfunk- und

WLAN-Stationen in der Nähe) von Microsoft anonymisiert in der Standortdatenbank gespeichert um die Standortermittlung zu verbessern.

- **Positionsdienste (Einstellung Nr. 2):** Wenn die Positionserkennung für das Gerät aktiviert ist, kann jeder Nutzer des Geräts über die Option Positionsdienste individuell festlegen, ob er den verwendeten Apps Zugang zu den Positionsdaten gewähren möchte.
- **Apps (Einstellung Nr. 3):** Sind sowohl die Positionserkennung als auch die Positionsdienste aktiviert, so kann für jede App, die Zugriff auf die Positionsdaten haben möchte, individuell festgelegt werden, ob dieser Zugriff gewährt werden soll.

Unsere Empfehlung: Sie sollten sowohl die Positionserkennung (Einstellung Nr. 1) als auch die Positionsdienste (Einstellung Nr. 2) ausschalten. Nur wenn Sie tatsächlich Apps verwenden möchten, bei denen der aktuelle Standort wichtig ist (bspw. Karten-App, Wetter-App,…), sollten Sie die Positionserkennung und Positionsdienste aktivieren. In diesem Fall sollten Sie aber nur jenen Apps Zugriff zu den Positionsdaten gewähren, die Sie tatsächlich verwenden! (Einstellung Nr. 3) Wenn Sie mehrere Apps installiert haben, sollten Sie von Zeit zu Zeit die Einstellungen in diesem Bereich kontrollieren und prüfen, ob die Einstellungen noch Ihren Vorstellungen entsprechen.

In der Kategorie „Kamera“ finden sich folgende Einstellungsmöglichkeiten:

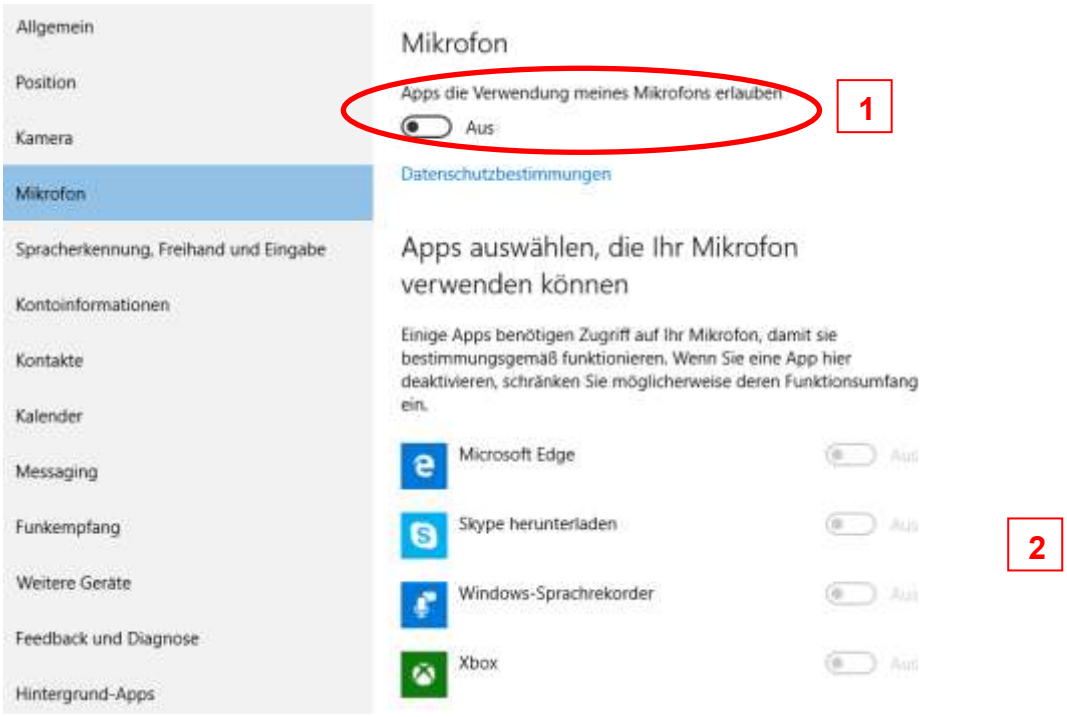


Erläuterungen zu den Datenschutzoptionen:

- **Erlauben (Einstellung Nr. 1):** Darüber lässt sich festlegen, ob Apps generell Zugriff auf die Kamera erhalten dürfen.
- **Apps (Einstellung Nr. 2):** Hier lässt sich explizit für jede App festlegen, ob sie Zugriff auf die Kamera erhalten darf.

  Unsere Empfehlung: Sie sollten Apps die Verwendung Ihrer Kamera nicht erlauben (Einstellung Nr. 1). Nur wenn Sie tatsächlich Apps benutzen, mit denen Sie die Kamera benutzen möchten (bspw. zur Video-Telefonie), sollten Sie Apps den Zugriff auf die Kamera erlauben und dann jeder App, der Sie keinen Zugriff auf die Kamera geben möchten, das Zugriffsrecht entziehen (Einstellung Nr. 2). Wenn Sie mehrere Apps installiert haben, sollten Sie von Zeit zu Zeit die Einstellungen in diesem Bereich kontrollieren und prüfen, ob die Einstellungen noch Ihren Vorstellungen entsprechen.

In der Kategorie „**Mikrofon**“ finden sich folgende Einstellungsmöglichkeiten:



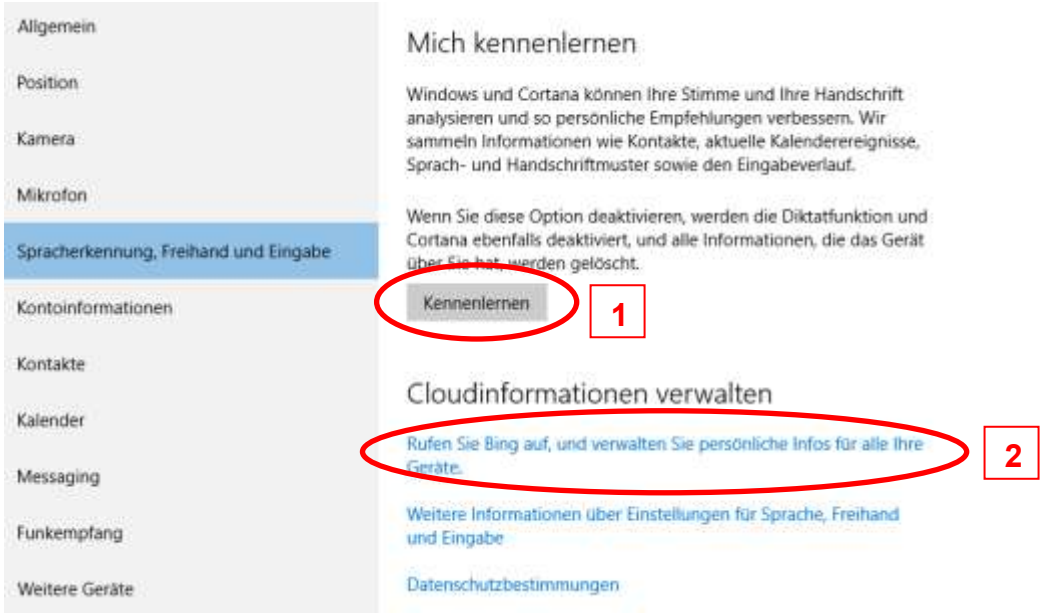
Erläuterungen zu den Datenschutzoptionen:

- **Erlauben (Einstellung Nr. 1):** Darüber lässt sich festlegen, ob Apps generell Zugriff auf das Mikrofon erhalten dürfen.
- **Apps (Einstellung Nr. 2):** Hier lässt sich explizit für jede App festlegen, ob sie Zugriff auf das Mikrofon erhalten darf.

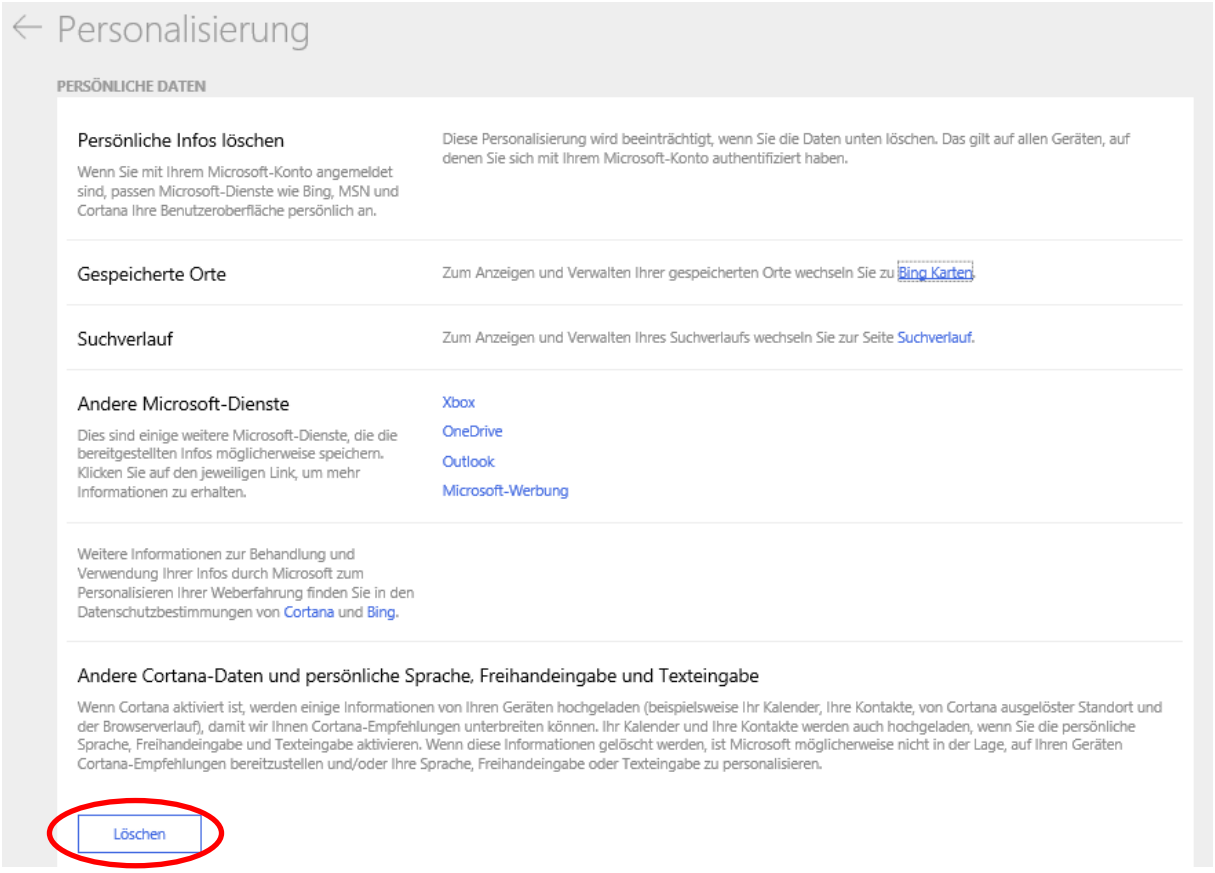
  Unsere Empfehlung: Sie sollten Apps die Verwendung Ihres Mikrofons nicht erlauben (Einstellung Nr. 1). Nur wenn Sie tatsächlich Apps benutzen, mit denen Sie das Mikrofon benutzen möchten (bspw. zur Telefonie), sollten Sie Apps den Zugriff auf das Mikrofon erlauben und dann jeder App, der Sie keinen Zugriff auf das Mikrofon geben möchten, das Zugriffsrecht entziehen (Einstellung Nr. 2). Wenn Sie mehrere Apps installiert haben, sollten Sie von Zeit zu Zeit die Einstellungen in diesem Bereich kontrollieren und prüfen, ob die Einstellungen noch Ihren Vorstellungen entsprechen.

In der Kategorie „**Spracherkennung, Freihand und Eingabe**“ können Sie festlegen, ob Sie den neuen, virtuellen Assistenten „Cortana“ verwenden möchten. Damit Cortana funktioniert, müssen Sie zum einen mit einem Microsoft-Konto auf Ihrem Rechner angemeldet sein und zum anderen müssen Sie dafür eine Reihe an persönlichen Daten an Microsoft senden. Unter anderem greift Microsoft auf Ihre Kontakte (inklusive Spitznamen), Kalenderereignisse, Interessen, Standorte, Eingabeverlauf, etc. zu. Des Weiteren werden Ihre Stimme und Ihr Handschriftmuster von Microsoft analysiert. Möchten Sie diese persönlichen Daten nicht an Microsoft senden, so achten Sie darauf, dass auf der grauen Schaltfläche „Kennenlernen“ steht, dann ist Cortana nicht aktiviert (Einstellung Nr. 1).

Unsere Empfehlung: Deaktivieren Sie Cortana! Sollte Cortana bei Ihnen standardmäßig bereits aktiviert sein, so klicken Sie auf die graue Schaltfläche „Kennenlernen beenden“. Sie müssen dann mit einem weiteren Klick bestätigen, dass Sie Cortana deaktivieren möchten.

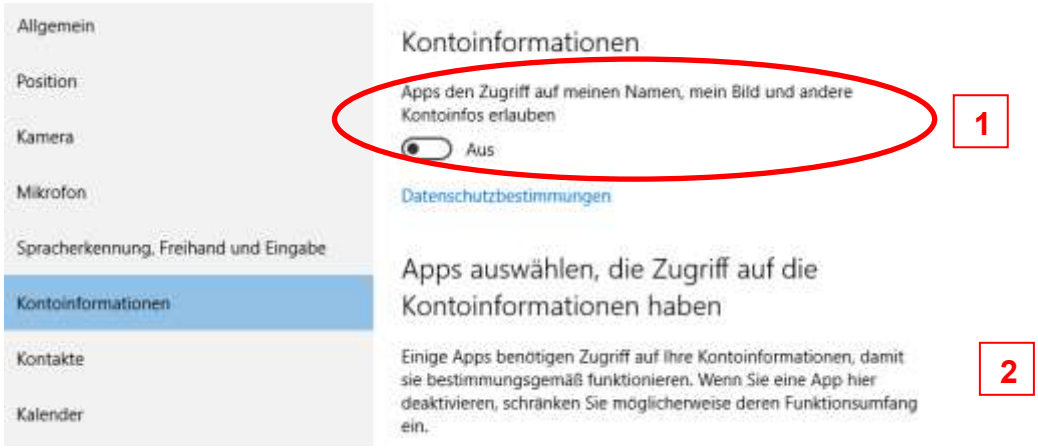


Als nächstes sollten Sie noch auf den Link „Rufen Sie Bing auf, und verwalten Sie persönliche Infos für alle Ihre Geräte“ (2) klicken. Sie werden dann auf eine Account-Personalisierungsseite von Bing geleitet:



Hier können Sie nun über die Schaltfläche „Löschen“ alle bereits an Microsoft gesendeten Daten (Kontakte, Kalendereinträge, Such- und Browserverlauf, etc.) löschen.
Microsoft verwendet leider nicht immer einheitliche Bezeichnungen für Einstellungen und Eigenschaften. „Orte“ bezeichnet in diesem Fall „Standorte“ (manchmal auch „Positionen“ genannt).

In der Kategorie „**Kontoinformationen**“ finden sich folgende Einstellungsmöglichkeiten:



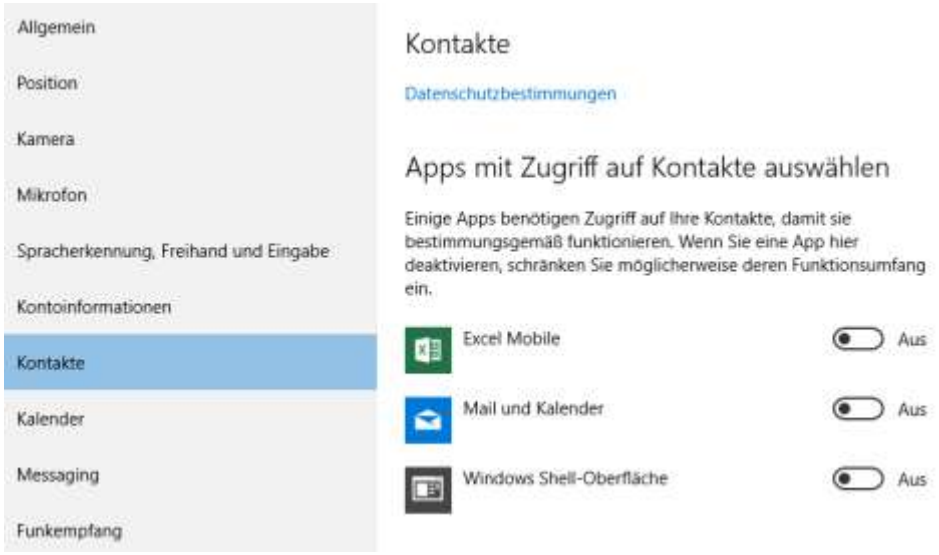
Erläuterungen zu den Datenschutzoptionen:

- **Erlauben (Einstellung Nr. 1):** Darüber lässt sich festlegen, ob Apps generell Zugriff auf Ihre Microsoft-Kontoinformationen erhalten dürfen.
- **Apps (Einstellung Nr. 2):** Hier lässt sich explizit für jede App festlegen, ob sie Zugriff auf die Microsoft-Kontoinformationen erhalten darf.

  Unsere Empfehlung: Sie sollten Apps den Zugriff auf Ihre Kontoinformationen nicht erlauben (Einstellung Nr. 1). Nur wenn Sie tatsächlich Apps benutzen, denen Sie Ihre Microsoft-Kontoinformationen zur Verfügung stellen möchten, sollten Sie Apps den Zugriff auf diese erlauben und dann jeder App, der Sie keinen Zugriff geben möchten, das Zugriffsrecht entziehen (Einstellung Nr. 2). Wenn Sie mehrere Apps installiert haben, sollten Sie von Zeit zu Zeit die Einstellungen in diesem Bereich kontrollieren und prüfen, ob die Einstellungen noch Ihren Vorstellungen entsprechen.

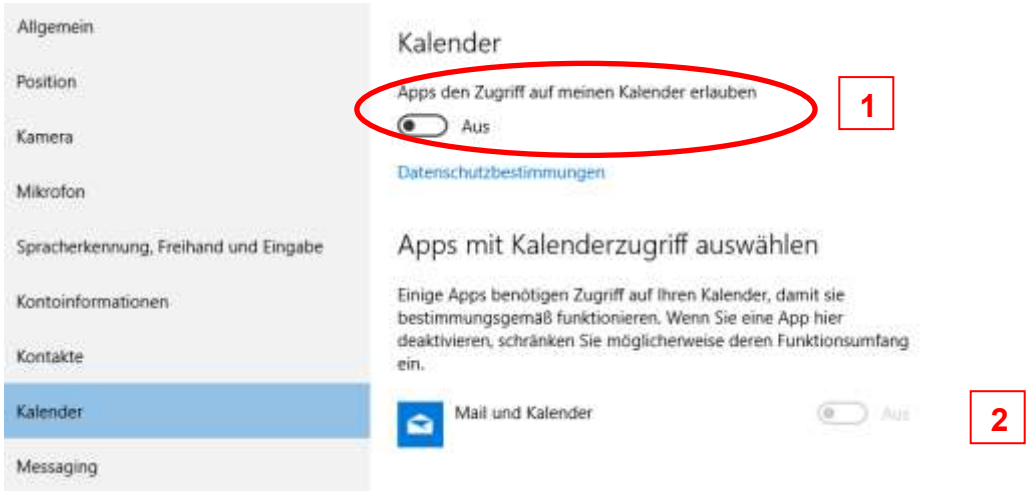
Allgemeine Informationen zu den Microsoft-Kontoinformationen finden Sie auch auf S. 20.

In der Kategorie „**Kontakte**“ können Sie festlegen, ob Sie Apps Zugriff auf Ihre Kontakte erlauben möchten.



Unsere Empfehlung: Blockieren Sie den Zugriff auf Ihre Kontakte für die Apps. Gewähren Sie nur ausgewählten Apps Zugriff auf Ihre Kontakte (bspw. der Mail-Anwendung).

In der Kategorie „**Kalender**“ können Sie festlegen, ob Sie Apps Zugriff auf Ihren Kalender erlauben möchten.

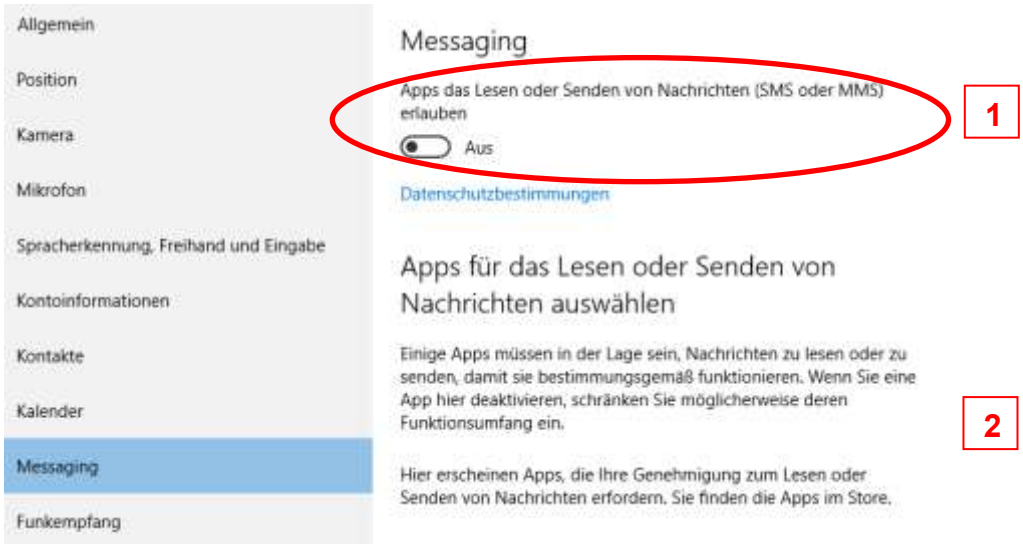


Erläuterungen zu den Datenschutzoptionen:

- **Erlauben (Einstellung Nr. 1):** Darüber lässt sich festlegen, ob Apps generell Zugriff auf den Kalender erhalten dürfen.
- **Apps (Einstellung Nr. 2):** Hier lässt sich explizit für jede App festlegen, ob sie Zugriff auf den Kalender erhalten darf.

  Unsere Empfehlung: Sie sollten Apps den Zugriff auf Ihren Kalender nicht erlauben (Einstellung Nr. 1). Nur wenn Sie tatsächlich Apps benutzen, mit denen Sie auf Ihren Kalender zugreifen möchten, sollten Sie Apps den Zugriff erlauben und dann jeder App, der Sie keinen Zugriff auf den Kalender geben möchten, das Zugriffsrecht entziehen (Einstellung Nr. 2). Wenn Sie mehrere Apps installiert haben, sollten Sie von Zeit zu Zeit die Einstellungen in diesem Bereich kontrollieren und prüfen, ob die Einstellungen noch Ihren Vorstellungen entsprechen.

In der Kategorie „**Messaging**“ können Sie festlegen, ob Sie Apps das Lesen oder Senden von Nachrichten (SMS) erlauben möchten. Diese Einstellung ist vor allem dann relevant, wenn Sie auf Ihrem Gerät eine Mobilfunkverbindung nutzen.

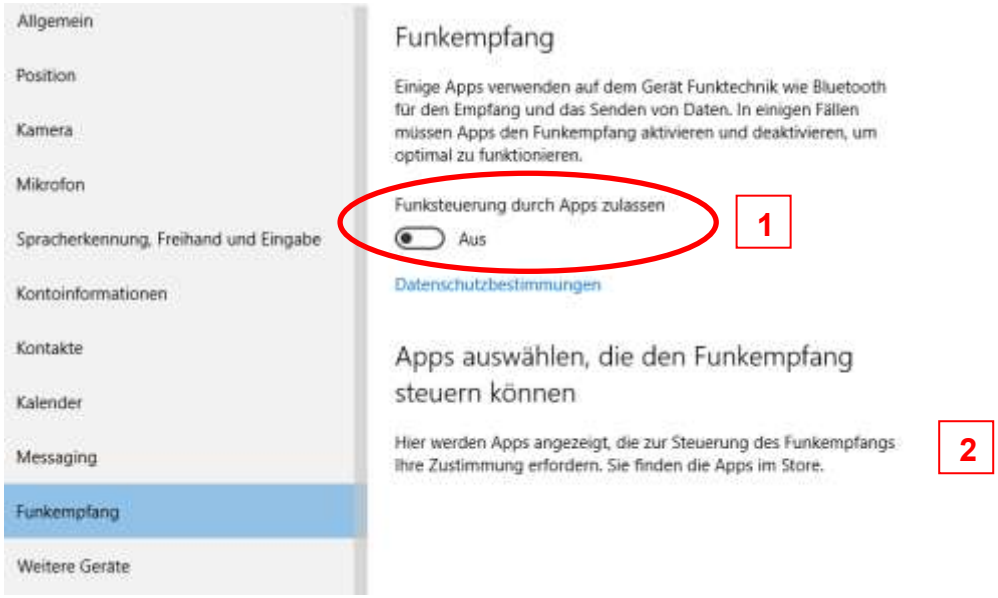


Erläuterungen zu den Datenschutzoptionen:

- **Erlauben (Einstellung Nr. 1):** Darüber lässt sich festlegen, ob Apps generell Nachrichten lesen/senden dürfen.
- **Apps (Einstellung Nr. 2):** Hier lässt sich explizit für jede App festlegen, ob sie Zugriff auf die SMS-Funktionalität erhalten darf.

  Unsere Empfehlung: Sie sollten Apps das Lesen oder Senden von Nachrichten nicht erlauben (Einstellung Nr. 1). Nur wenn Sie tatsächlich Apps benutzen, mit denen Sie SMS lesen bzw. senden möchten, sollten Sie Apps den Zugriff erlauben und dann jeder App, der Sie keinen Zugriff geben möchten, das Zugriffsrecht entziehen (Einstellung Nr. 2). Hier gilt es auch zu bedenken, dass böswillige Apps, denen das Senden von SMS erlaubt wird, auch Mehrwert-Dienste in Anspruch nehmen können, wodurch Ihnen höhere Telefonkosten entstehen können. Wenn Sie mehrere Apps installiert haben, sollten Sie von Zeit zu Zeit die Einstellungen in diesem Bereich kontrollieren und prüfen, ob die Einstellungen noch Ihren Vorstellungen entsprechen.

In der Kategorie „**Funkempfang**“ können Sie festlegen, ob Sie Apps Zugriff auf die Funkeinheit erlauben möchten.

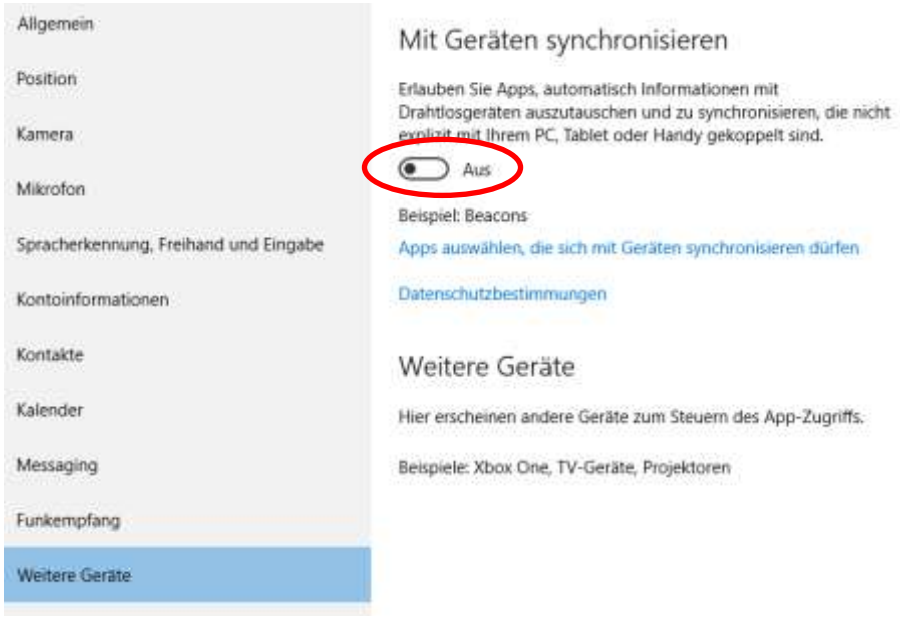


Erläuterungen zu den Datenschutzoptionen:

- **Erlauben (Einstellung Nr. 1):** Darüber lässt sich festlegen, ob Apps generell die Funksteuerung ändern und per Funk Daten senden und empfangen dürfen.
- **Apps (Einstellung Nr. 2):** Hier lässt sich explizit für jede App festlegen, ob sie Zugriff auf die Funkeinheit erhalten darf.

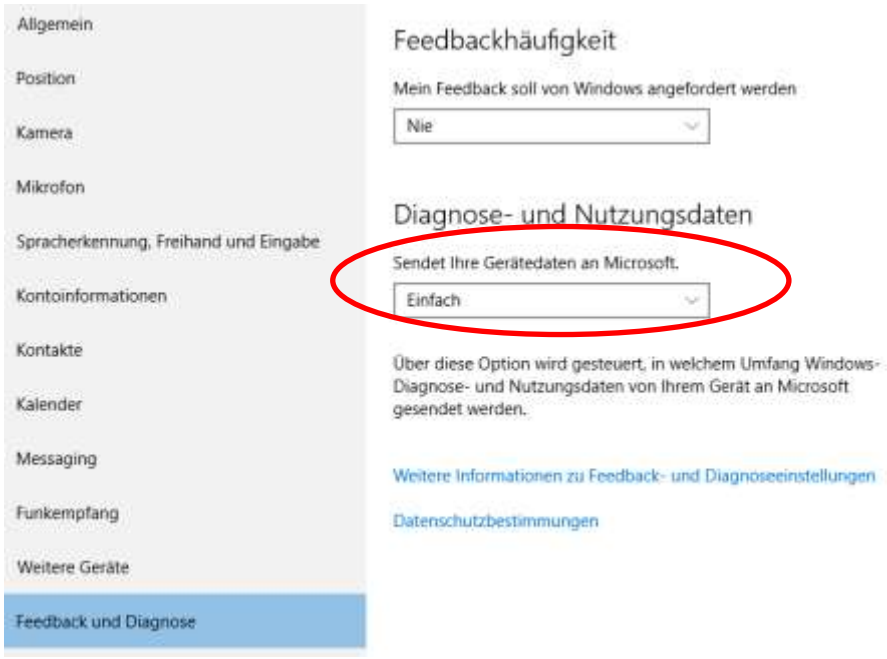
  Unsere Empfehlung: Sie sollten Apps die Verwendung der Funksteuerung nicht erlauben (Einstellung Nr. 1). Nur wenn Sie tatsächlich Apps benutzen, mit denen Sie Daten per Funkeinheit (bspw. Bluetooth) zu anderen Geräten senden bzw. von diesen empfangen, sollten Sie Apps den Zugriff erlauben und dann jeder App, der Sie keinen Zugriff geben möchten, das Zugriffsrecht entziehen (Einstellung Nr. 2). Wenn Sie mehrere Apps installiert haben, sollten Sie von Zeit zu Zeit die Einstellungen in diesem Bereich kontrollieren und prüfen, ob die Einstellungen noch Ihren Vorstellungen entsprechen.

In der Kategorie „**Weitere Geräte**“ können Sie festlegen, ob Apps automatisch Daten mit anderen Geräten (bspw. XBox One, TV-Geräte, etc.) austauschen dürfen. Die Datenschutzbestimmungen finden sich hierzu nur auf den betroffenen Apps/Geräte-Webseiten, weshalb wir die Auswirkungen nicht allgemein überprüfen können.



Unsere Empfehlung: Deaktivieren Sie diese Funktion.

In der Kategorie „**Feedback und Diagnose**“ können Sie zum einen festlegen, wie häufig Microsoft Sie um Feedback fragen darf, und zum anderen, in welchem Umfang Sie Daten über Ihre Windows-Nutzung an Microsoft senden möchten.



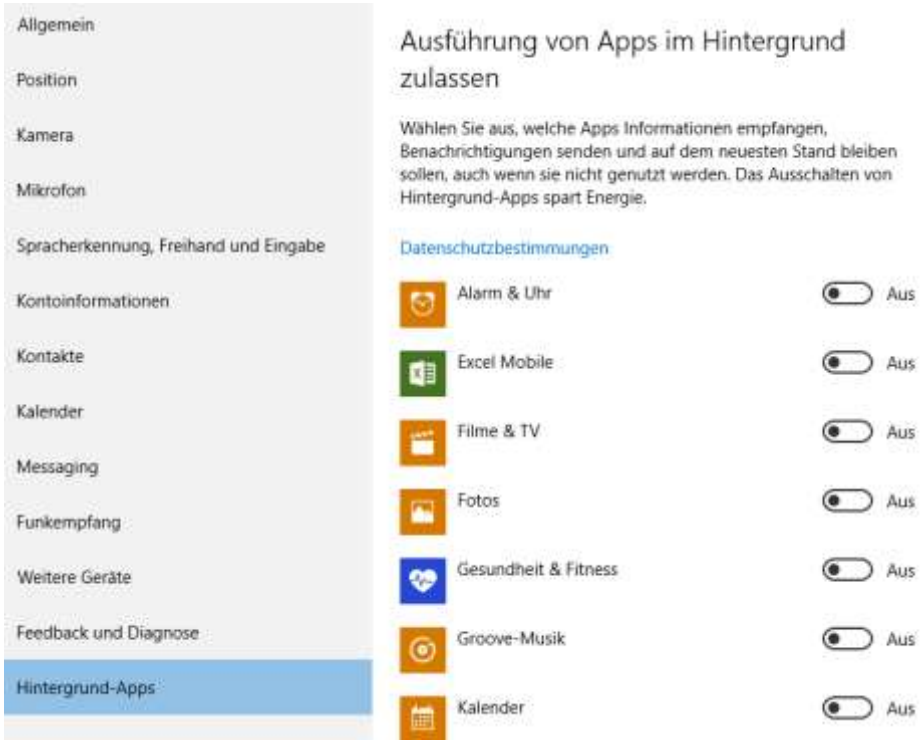
Aus Datenschutzsicht ist vor allem die Einstellung unter Diagnose- und Nutzungsdaten interessant. Hier gibt es die folgenden Möglichkeiten:

- **Einfach:** Bei dieser Einstellung werden Informationen zum verwendeten Gerät (Prozessortyp, Massenspeichergröße, Bildschirm-Auflösung, eindeutig identifizierende Nummer des Mobilfunkgeräts (IMEI)), Daten zu System- und Anwendungsabstürzen und Informationen zum Systemzustand (installierte Anwendungen/Apps, installierte Treiberversionen, installierte Updates) an Microsoft gesendet. Diese Informationen werden von Microsoft verwendet um zu ermitteln, welche Updates an das System übermittelt werden sollen.
- **Verbessert:** Bei dieser Einstellung werden zusätzlich zu den Daten, die bei der Einstellung „Einfach“ an Microsoft übermittelt werden, auch noch Hauptspeicherabbilder bei Systemabstürzen mit übermittelt. In den Hauptspeicherabbildern können personenbezogene Daten, Dokumente, an denen Sie kurz vor dem Absturz gearbeitet haben, sowie Passwörter oder kryptographische Schlüssel enthalten sein.
- **Vollständig:** Bei dieser Einstellung – die von Microsoft empfohlen wird – werden alle Daten, die auch bei den Einstellungen „Einfach“ und „Verbessert“ gesendet werden, an Microsoft übermittelt. Zusätzlich ist es möglich, dass sich ein Microsoft-Mitarbeiter mit Ihrem Rechner verbindet und über Fernwartung versucht, Ihre Computer-Probleme zu lösen. Damit kann der Microsoft-Mitarbeiter Zugriff auf Ihre persönlichen Daten erhalten.

  Unsere Empfehlung: Verwenden Sie die Einstellung „Einfach“, da dies die datensparsamste Einstellung darstellt. Bitte beachten Sie, dass auch bei dieser Einstellung Daten an Microsoft gesendet werden – vollständig lässt sich die Datenübermittlung nicht abstellen. Laut Datenschutzbestimmungen werden die gesammelten Daten von Microsoft, sowie seinen Lieferanten und

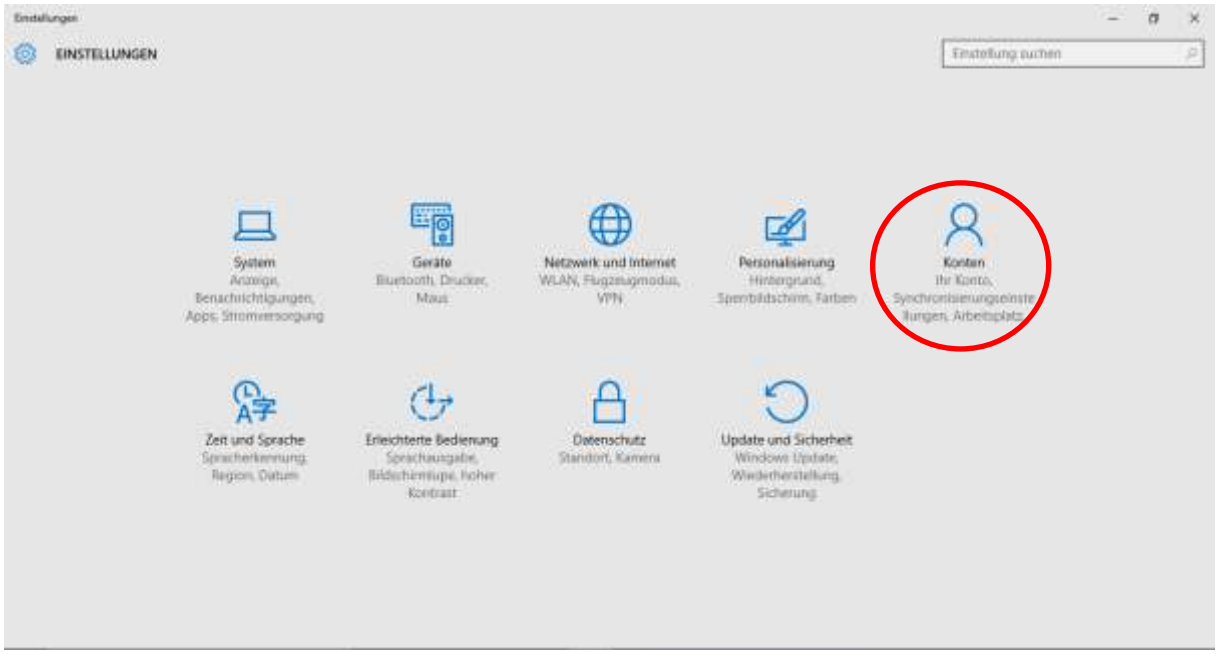
Partnern, ausschließlich zur Problembehandlung und Weiterentwicklung von Produkten (Software/Hardware/Dienstleistungen) verwendet. Die Daten würden lt. Microsoft nicht für gezielte Werbung verwendet.

In der Kategorie „**Hintergrund-Apps**“ lässt sich konfigurieren, welche Apps im Hintergrund Informationen senden und empfangen dürfen.

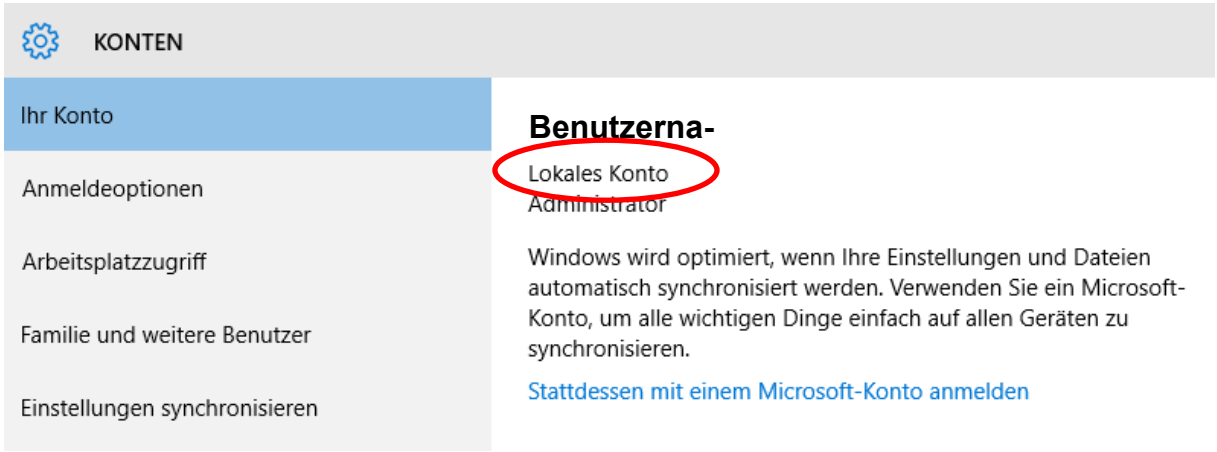


Unsere Empfehlung: Sie sollten das Senden und Empfangen von Daten für Apps im Hintergrund nicht erlauben. Nur für einzelne Apps, wenn Sie die Informationen dieser Apps auch tatsächlich benötigen (bspw. das aktuelle Wetter an Ihrem Standort bei der Wetter-App), sollten Sie das Senden und Empfangen erlauben.

Nachdem Sie die allgemeinen Datenschutz-Einstellungen von Windows 10 vorgenommen haben, sollten Sie noch die Datenschutzeinstellungen für Ihr Benutzer-Konto überprüfen. Dazu wählen Sie unter „Einstellungen“ – „Konten“ aus.

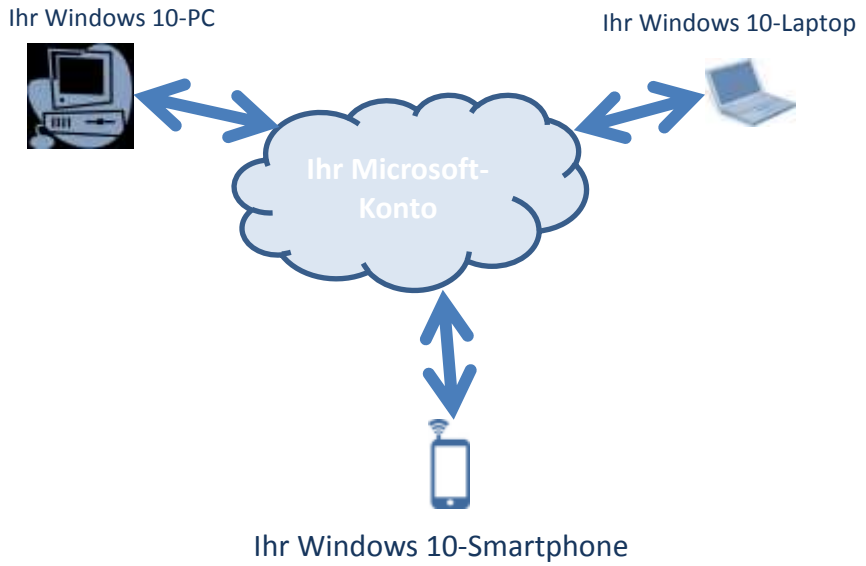


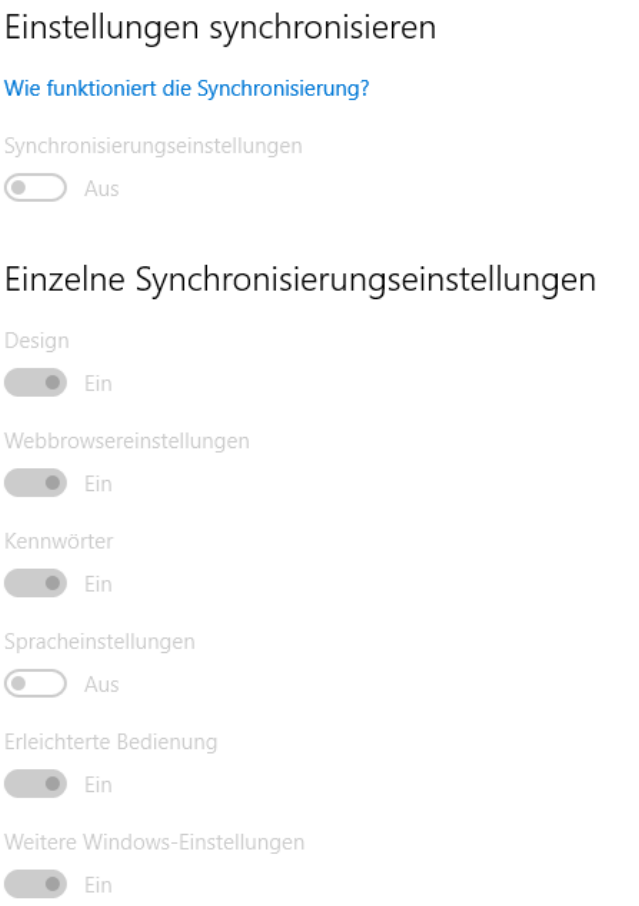
Prüfen Sie zunächst, ob Sie ein lokales Nutzerkonto zur Anmeldung am Rechner verwenden. Dazu muss unter Ihrem Benutzername „Lokales Konto“ stehen. Ist dies nicht der Fall, so klicken Sie auf „Stattdessen mit einem lokalen Konto anmelden“. Dann legen Sie entweder ein neues, lokales Benutzerkonto an oder melden sich mit dem lokalen Benutzerkonto an, das Sie bei der Installation von Windows 10 eingerichtet haben.



Was Sie bei der Anmeldung mit einem Microsoft-Benutzerkonto wissen müssen:
Einige Dienste von Microsoft funktionieren nur, wenn Sie sich mit einem Microsoft-Benutzerkonto an Ihrem Rechner anmelden. Bspw. können Sie auf die OneDrive-Cloud sowie den App Store nur zugreifen, wenn Sie mit einem Microsoft-Benutzerkonto angemeldet sind. Möchten Sie diese Dienste nutzen, so melden Sie sich mit Ihrem Microsoft-Benutzerkonto an. In diesem Fall empfehlen wir Ihnen die folgenden Datenschutz-Einstellungen vorzunehmen. Dazu klicken Sie unter „Einstellungen“ – „Konten“ in der linken Liste auf den Eintrag „**Einstellungen synchronisieren**“.

Im Folgenden können Sie festlegen, welche Einstellungen synchronisiert werden sollen. Die Synchronisierung soll sicherstellen, dass Sie dieselben Einstellungen auf all Ihren Geräten die mit Windows laufen (bspw. Smartphone und PC), vorfinden. Es ist zu beachten, dass die Daten dafür an Microsoft gesendet und dort gespeichert werden. Die Synchronisation zwischen Ihren Windows 10-Geräten läuft über die Microsoft-Cloud:

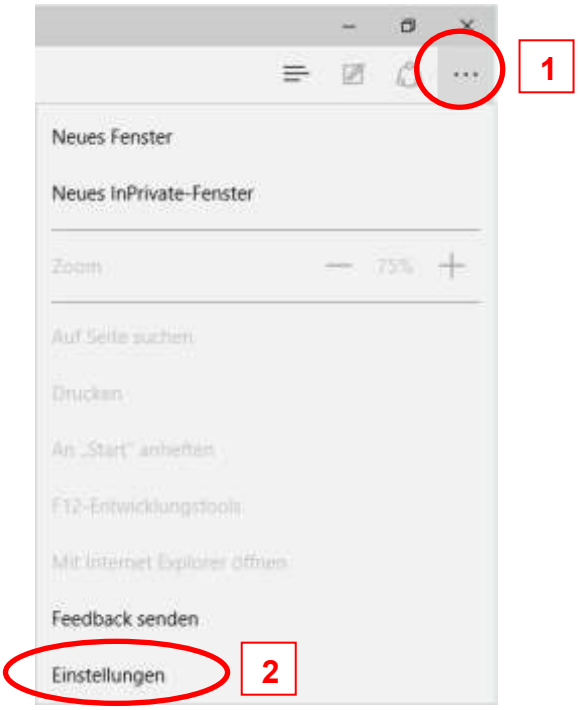




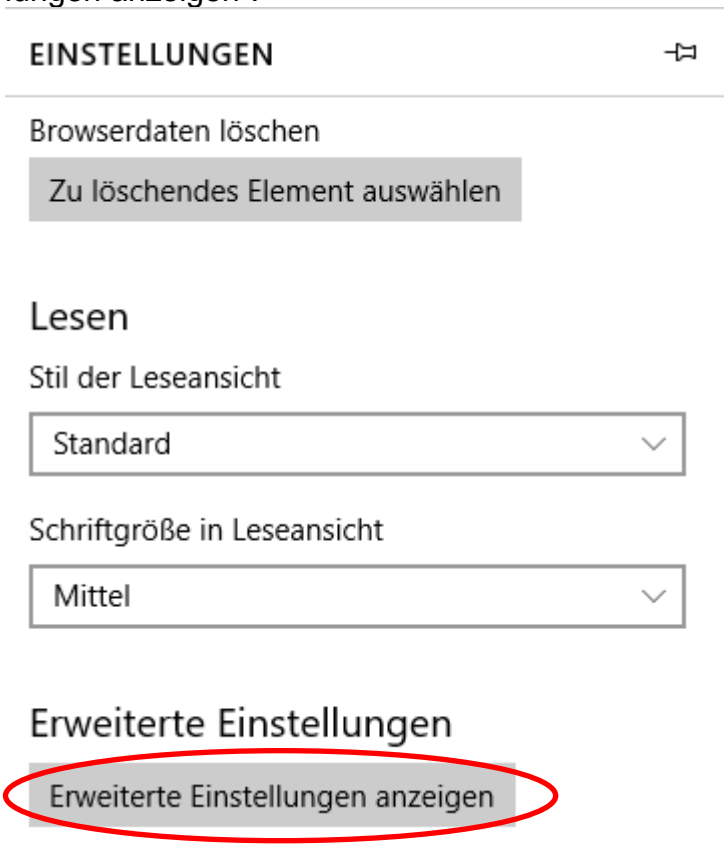
In den Datenschutzbestimmungen werden die einzelnen Punkte nicht näher erläutert. Bei den Webbrowsereinstellungen sind u. a. der Web-Browser-Verlauf, die Favoriten und Webseiten, die Sie geöffnet haben, mit inbegriffen. Bei den Kennwörtern werden bspw. auch die WLAN-Kennwörter mit synchronisiert.

Unsere Empfehlung: Sie sollten möglichst wenige Einstellungen synchronisieren, da die Daten auf Microsoft-Servern gespeichert werden. Vor allem sollten Sie Abstand davon nehmen, Ihre Webbrowsereinstellungen zu synchronisieren, da diese sehr persönliche Daten beinhalten!

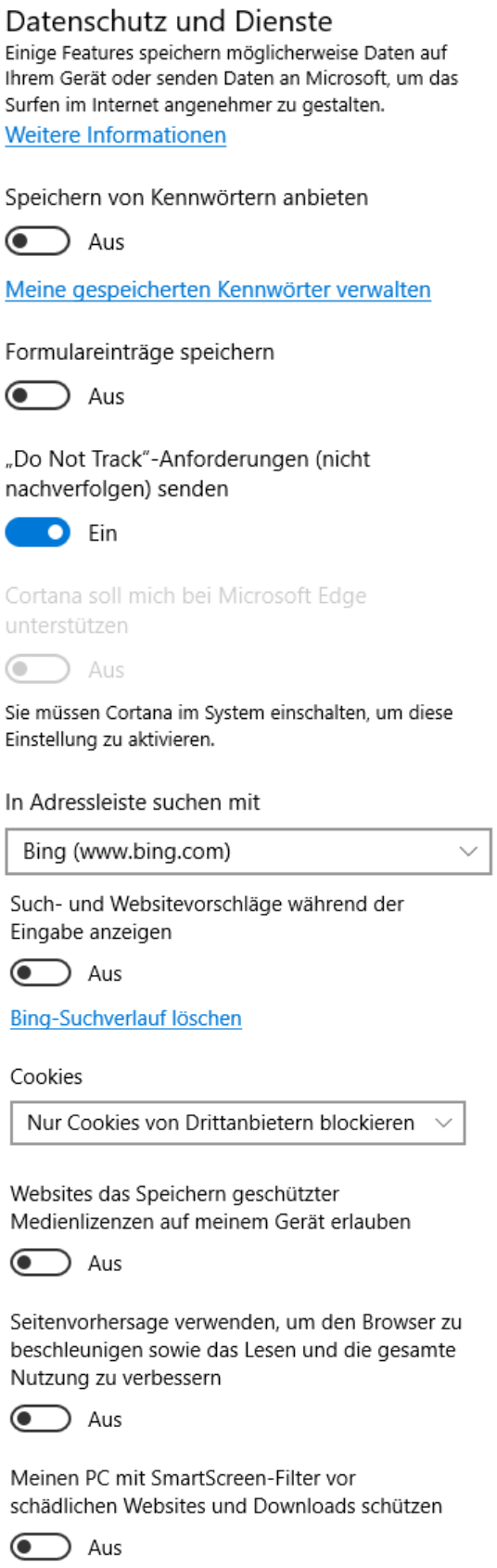
Im letzten Schritt sollten im neuen Browser „**Edge**“ noch einige Datenschutzeinstellungen vorgenommen werden. Dazu klicken Sie im Browser rechts oben auf die drei kleinen Punkte (Schritt 1) und als nächstes auf „Einstellungen“ (Schritt 2).



Im nun erscheinenden Dialogfenster klicken Sie auf den Eintrag „Erweiterte Einstellungen anzeigen“.



Danach scrollen Sie bis zum Bereich „Datenschutz und Dienste“.



Unsere Empfehlung: Hier sollte man vier Einstellungen vornehmen:

- „Do Not Track“-Anforderung senden einschalten.
- Cookies: „Nur von Drittanbietern blockieren“ auswählen. Dies erschwert ein Tracking über mehrere Webangebote hinweg.
- „Seitenvorhersage“ abschalten. Ansonsten werden die besuchten Webseiten an Microsoft gesendet und Microsoft ermittelt auf dieser Grundlage jene Webseiten, die Sie wahrscheinlich als nächstes abrufen werden.
- „SmartScreen-Filter“ deaktivieren (siehe dazu die Erklärung auf S. 3).