

# Windows 10 - Datenschutzkonfiguration

## Tools zu Konfiguration von Windows 10

Hilfe beim Deaktivieren der datenschutzrechtlich bedenklichen Einstellungen und Dienste, die unbedingt vorgenommen werden sollten, erhält man durch Tools, die mit einer einheitlichen und übersichtlichen Oberfläche eine gesicherte Umgebung einrichten können. Sie bieten den Vorteil, dass man nur eine Oberfläche zur kompletten Konfiguration benötigt. Außerdem kann man die gewünschten Einstellungen in einem File exportieren und dieses nach jedem Update wieder importieren. Damit spart man sich nicht nur Zeit, sondern stellt damit sicher, dass man die Datenschutzeinstellungen vollständig vornimmt.

Wir testeten das **ShutUp10** Tool:

- \* Das Tool ist Freeware. Es wird aber momentan empfohlen, nicht über die Hersteller-Webseite herunterzuladen, da man seine Mailadresse angeben muss. Man kann es aber problemlos von bspw. folgender Seite herunterladen: <https://www.oo-software.com/de/shutup10>
- \* Die Einstellungen des Tools müssen mit der Zeit überprüft werden. Empfehlenswert ist ein solches Tool mindestens zweimal jährlich oder nach jedem Update durchzuführen.
- \* Sie können auch die Einstellungen des Tools exportieren, um sie dann bei sich und anderen Benutzern schnell nachtragen und/oder wiederholen zu können.
- \* Bitte beachten Sie, dass die Tools selbst mit jedem neuen Update auf Ihre Sicherheit überprüft werden sollten. Wenn Sie diesbezüglich unsicher sein sollten, wenden Sie sich an Ihren Administrator.

Vom ZENDAS wird das Tool **W10Privacy** empfohlen:

- \* Das Tool kann direkt beim Hersteller gedownloadet werden: <http://www.winprivacy.de>
- \* Auch hier kann man eine Konfigurationsdatei anlegen und diese nach jedem Update wieder einspielen.

Das BSI hat im Juni 2022 eine aktuelle Anleitung zu Deaktivierung der Telemetrie in Windows 10 21H2 bereitgestellt! S. hier: <https://downloads.rz.uni-freiburg.de/freier-zugang/software/bsi-anleitung-deaktivierung-der-telemetrikomponente-in-windows-10-21h2/>

## Einstellungen über die Gruppenrichtlinien

Viele Einstellungen können auch über die Gruppenrichtlinien vorgenommen werden.

Die Gruppenrichtlinien sollten nur von erfahrenen Usern bearbeitet werden!

Einige Einstellungen finden Sie in den Gruppenrichtlinien unter folgenden Kategorien:

Benachrichtigungen auf Sperrbildschirm deaktivieren

Computerkonfiguration

- > Administrative Vorlagen
- > Systemsteuerung
- > Anpassung
- > Ein bestimmtes Standardbild für den Sperr- und Anmeldebildschirm erzwingen

Häkchen bei "Unterhaltung Tipps, Tricks und mehr auf dem Sperrbildschirm" entfernen

Updates aus anderen Quellen deaktivieren

- Computerkonfiguration
- > Administrative Vorlagen
  - > Windows-Komponenten
  - > Übermittlungsoptimierung

Option: Keine

Deaktivierung Windows-Store

- Computerkonfiguration
- > Administrative Vorlagen
  - > Windows-Komponenten
  - > Store
- Einstellung Alle Apps aus Windows Store deaktivieren

Synchronisation der Einstellungen unterbinden

- Computerkonfiguration
- > Administrative Vorlagen
  - > Windows-Komponenten
  - > Einstellungen synchronisieren
- Einstellung Nicht synchronisieren

Zugriff auf Nachrichten (SMS oder MMS) durch Apps unterbinden

- Gruppenrichtlinie Computerkonfiguration
- > Administrative Vorlagen
  - > Windows-Komponenten
  - > Datenschutzbestimmungen für die App
- Einstellung Zugriff auf Messaging durch Windows-Apps zulassen  
Wert Legen Sie das Feld "Eine Einstellung wählen" als "Force Deny" fest

- Zugriff auf Kalender durch Apps unterbinden
- Gruppenrichtlinie Computerkonfiguration
- > Administrative Vorlagen
  - > Windows-Komponenten
  - > Datenschutzbestimmungen für die App
- Einstellung Zugriff auf den Kalender durch Windows-Apps zulassen  
Wert Legen Sie das Feld "Eine Einstellung wählen" als "Force Deny" fest

Zugriff auf Kontaktdaten durch Apps unterbinden

### Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows-Komponenten

> Datenschutzbestimmungen für die App

Einstellung Zugriff auf Kontaktdaten durch Windows-Apps zulassen

Wert Legen Sie das Feld "Eine Einstellung wählen" als "Force Deny" fest

Zugriff auf Kontoinformationen durch Apps unterbinden

### Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows-Komponenten

> Datenschutzbestimmungen für die App

Einstellung Zugriff auf Kontoinformationen durch Windows-Apps zulassen

Wert Legen Sie das Feld "Eine Einstellung wählen" als "Force Deny" fest

Handschrifterkennung deaktivieren

### Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Systemsteuerung

> Regions- und Sprachoptionen

> Handschriftenanpassung

Einstellung Automatisches Lernen deaktivieren

Zugriff auf Mikrofon durch Apps unterbinden

### Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows-Komponenten

> Datenschutzbestimmungen für die App

Einstellung Zugriff auf das Mikrofon durch Windows-Apps zulassen

Beschreibung

(GPO)

Legen Sie das Feld "Eine Einstellung wählen" als "Force Deny" fest./.

Zugriff auf Kamera durch Apps unterbinden

### Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows-Komponenten

> Datenschutzbestimmungen für die App

Einstellung Zugriff auf die Kamera durch Windows-Apps zulassen

Beschreibung

(GPO)

Legen Sie das Feld "Eine Einstellung wählen" als "Force Deny" fest./.

Zugriff auf Positionsdaten durch Apps unterbinden

### Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows-Komponenten

> Datenschutzbestimmungen für die App

Einstellung Zugriff auf Positionsdaten durch Windows-Apps zulassen

Beschreibung

(GPO)

Legen Sie das Feld "Eine Einstellung wählen" als "Force Deny" fest./.

Positionsskripting von Programmen unterbinden

Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows-Komponenten

> Position und Sensoren

Einstellung Positionsskripting deaktivieren

Wert Aktiviert

Sensorfeature deaktivieren

Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows-Komponenten

> Position und Sensoren

Einstellung Sensoren deaktivieren (ABER: Lichtsensoren für automatische Einstellung der Bildschirmhelligkeit)

Speicherort für Postition deaktivieren

Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows-Komponenten

> Position und Sensoren

Einstellung Speicherort deaktivieren

Wert Aktiviert

Experimentiermodus abschalten

Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows Komponenten

> Datensammlung und Vorabversionen

Einstellung Features oder Einstellungen der Vorabversion deaktivieren

Wert Deaktiviert

Suchvorschläge auf Adressleiste anzeigen

Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows Komponenten

> Microsoft Edge

Einstellung Blockiert die Anzeige von Suchvorschlägen auf der Adressleiste

Wert Deaktiviert

Passwort-Manager im Browser

Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows Komponenten

> Microsoft Edge

Einstellung Ermöglicht das Konfigurieren des Kennwort-Managers

Wert Deaktiviert

"Do Not Track"-Anforderung an Webseiten senden

### Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows Komponenten

> Microsoft Edge

Einstellung Ermöglicht Ihnen, Benutzern das Senden von DNT-Kopfzeilen zu erlauben

Wert Aktiviert

### Autoausfüllen-Funktion auf Webseiten

Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows Komponenten

> Microsoft Edge

Einstellung Ermöglicht Ihnen, Benutzern die Verwendung von AutoAusfüllen auf Websites zu erlauben

Wert Deaktiviert

### von Webseiten angeforderte Positionsdaten vom Browser

Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows Komponenten

> Internet Explorer

Einstellung Browser-Geolocation deaktivieren

Wert Aktiviert

### Periodische Suche nach Browser-Updates

Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows Komponenten

> Internet Explorer

Einstellung Periodische Überprüfungen auf Internet Explorer-Softwareupdates deaktivieren

Wert Aktiviert

### Autovervollständigung für Webadressen

Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows Komponenten

> Internet Explorer

Einstellung AutoVervollständigen für Webadressen deaktivieren

Wert Aktiviert

### Suchvorschläge für Microsoftdienste deaktivieren

Gruppenrichtlinie Computerkonfiguration

> Administrative Vorlagen

> Windows Komponenten

> Internet Explorer

Einstellung Für Microsoft-Dienste das Bereitstellen von erweiterten Vorschlägen

zulassen, wenn Benutzer Text in die Adressleiste eingeben

Wert Deaktiviert

### Seitenvorschläge im Internet Explorer deaktivieren

Gruppenrichtlinie Computerkonfiguration

- > Administrative Vorlagen
- > Windows Komponenten
- > Internet Explorer

Einstellung "Vorgeschlagene Sites" aktivieren

Wert Deaktiviert

### Insider Builds deaktivieren

Gruppenrichtlinie Computerkonfiguration

- > Administrative Vorlagen
- > Windows Komponenten
- > Datensammlung und Vorabversionen

Einstellung Benutzersteuerung für Insider-Builds ein-/ausschalten

Wert Deaktiviert

### Weitergabe von Informationen im Suchvorgang an Bing deaktivieren

Gruppenrichtlinie Computerkonfiguration

- > Administrative Vorlagen
- > Windows Komponenten
- > Suche

Einstellung Festlegen der in der Suche freizugebenden Informationen

Wert Aktiviert - Anonyme Informationen

### Websuche mit Cortana deaktivieren

Gruppenrichtlinie Computerkonfiguration

- > Administrative Vorlagen
- > Windows Komponenten
- > Suche

Einstellung Nicht im Web suchen und keine Webergebnisse in der Suche anzeigen

Wert Aktiviert

### Websuche für Desktopsuche deaktivieren

Gruppenrichtlinie Computerkonfiguration

- > Administrative Vorlagen
- > Windows Komponenten
- > Suche

Einstellung Websuche nicht zulassen

Wert Aktiviert

### Nutzung von Positionsdaten deaktivieren

Gruppenrichtlinie Computerkonfiguration

- > Administrative Vorlagen
- > Windows Komponenten
- > Suche

Einstellung Der Suche und Cortana die Nutzung von Positionsdaten verbieten

Wert Deaktiviert

### Blockierte ActiveX-Steuerelementen - Download von aktualisierten

Listen deaktivieren

```
REG_DWORD-Registrierungseinstellung:  
HKEY_CURRENT_USER\Software\Microsoft\Internet  
Explorer\VersionManager\DownloadVersionList  
> Wert auf "0" stellen
```

### Konfiguration über die Powershell

Einige Einstellungen können auch über die Powershell vorgenommen werden.

Folgende Befehle können Abhilfe schaffen:

```
New-ItemProperty -path "HKLM\  
SOFTWARE\Policies\Microsoft\Windows\DataCollection" -name  
"AllowTelemetry" -value "0" -propertyType dword -force  
  
New-ItemProperty -path  
"HKLM\SOFTWARE\Policies\Microsoft\Windows\OneDrive" -name  
"DisableFileSyncNGSC" -value "1" -propertyType dword -force  
  
New-ItemProperty -path  
"HKLM\SOFTWARE\Policies\Microsoft\Windows\  
LocationAndSensors" -name "DisableWindowsLocationProvider"  
-value "1" -propertyType dword -force  
  
New-ItemProperty -path  
"HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows Search"  
-name "AllowCortana" -value "0" -propertyType dword -force  
  
New-ItemProperty -path  
"HKLM\SOFTWARE\Policies\Microsoft\Windows\Device Metadata"  
-name "PreventDeviceMetadataFromNetwork" -value "1" -  
propertyType dword -force  
  
New-ItemProperty -path  
"HKLM\SOFTWARE\Policies\Microsoft\MRT" -name  
"DontOfferThroughWUAU" -value "1" -propertyType dword  
-force  
  
oder  
  
New-ItemProperty -path  
"HKLM\SOFTWARE\Policies\Microsoft\MRT" -name "  
DontReportInfectionInformation " -value "1" -propertyType  
dword -force  
  
New-ItemProperty -path  
"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet"  
-name " SubmitSamplesConsent" -value "0" -propertyType  
dword -force
```

```
New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\Windows Defender\Spynet"
-name "SpyNetReporting" -value "0" -propertyType dword
-force

New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\SQMClient\Windows" -name
"CEIPEnable" -value "0" -propertyType dword -force

New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\Windows\AppCompat" -name
"AITEnable" -value "0" -propertyType dword -force

New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\Windows\AppCompat" -name
"DisableInventory" -value "1" -propertyType dword -force

Get-Service DiagTrack | Set-Service -StartupType Disabled

Get-Service DiagTrack | Set-Service -StartupType Disabled

New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\Windows\AdvertisingInfo"
-name "DisabledbyGroupPolicy" -value "1" -propertyType
dword -force

New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\Windows\System" -name
"EnableSmartScreen" -value "0" -propertyType dword -force

New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\MicrosoftEdge\
PhishingFilter" -name "EnabledV9" -value "0" -propertyType
dword -force

New-ItemProperty -path "HKCU\SOFTWARE\Microsoft\Input\TIPC"
-name "Enabled" -value "0" -propertyType dword -force

New-ItemProperty -path "HKCU\Control
Panel\International\User Profile" -name
"httpAcceptLanguageOptOut" -value "1" -propertyType dword
-force

New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\Windows\System" -name
"AllowUserInfoAccess" -value "2" -propertyType dword -force

oder

New-ItemProperty -path
"HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\DeviceAcces
```



```
s\Global\{C1D23ACC-752B-43E5-8448-8D0E519CD6D6}" -name
"Value" -value "Deny" -propertyType string -force

New-ItemProperty -path
"HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\
DeviceAccess\Global\{A8804298-2D5F-42E3-9531-9C8C39EB29CE}"
-name "Value" -value "Deny" -propertyType string -force

New-ItemProperty -path
"HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\
DeviceAccess\Global\LooselyCoupled" -name "Value" -value
"Deny" -propertyType string -force

New-ItemProperty -path "HKCU\SOFTWARE\Microsoft\Siuf\Rules"
-name "PeriodInNanoSeconds" -value "0" -propertyType
dword -force

oder

New-ItemProperty -path "HKCU\SOFTWARE\Microsoft\Siuf\Rules"
-name "NumberOfSIUFInPeriod" -value "0" -propertyType
dword -force

New-ItemProperty -path
"HKLM\SOFTWARE\Policies\Microsoft\Windows\Windows Error
Reporting" -name "Disabled" -value "1" -propertyType dword
-force

New-ItemProperty -path "HKLM\
SOFTWARE\Microsoft\WcmSvc\wifinetworkmanager\config" -name
"AutoConnectAllowedOEM" -value "0" -propertyType dword -
force

Get-AppxPackage *bingnews* | Remove-AppxPackage
Get-AppxProvisionedPackage -online | where {$_.displayname
-match "skype"} | Remove-AppxProvisionedPackage -online

Get-AppxPackage *bingweather* | Remove-AppxPackage

Get-AppxPackage *bingfinance* | Remove-AppxPackage

Get-AppxPackage *bingSports* | Remove-AppxPackage
```

[Beschaffung - Artikelübersicht](#), [Software - Artikelübersicht](#), [Windows - Artikelübersicht](#), [Sicherheit - Artikelübersicht](#)

From:

<https://www.wiki.uni-freiburg.de/rz/> - **RZ**

Permanent link:

[https://www.wiki.uni-freiburg.de/rz/doku.php?id=windows\\_10](https://www.wiki.uni-freiburg.de/rz/doku.php?id=windows_10)



Last update: **2022/06/05 13:10**