Check-list
Data protection under Windows 10

Windows 10 analyses various personal data. Data affected here are for instance your e-mail address and contents of e-mails received and sent out, personal interests and favourites, purchase and payment data, your personal address book, etc.

Many of these data are also transmitted to Microsoft. Most of these data transmission mechanisms however can be switched off. On the one hand, you should consider certain criteria when first installing (updating) Windows 10; on the other, various settings can still be adjusted afterwards. Our check-list is meant to assist you with selecting the correct settings and to protect your data and all your private information in the best possible way.

We have tried to draw up as universally applicable a set of instructions for private users as possible. Nevertheless, the individual configuration options and settings may differ in specific cases. This check-list refers to the options available as at **29th May 2018**.

The «OK» column provides an option to tick all settings already checked and adjusted.

Settings during Windows 10 installation (update)

During any Windows 10 installation (update), the different data protection setting options are displayed on a page entitled «Choose privacy settings for your device», with a clear explanation given for every setting as to what it is for. By default, all settings are set to «on».

To prevent Windows from sending too many data unintentionally, you should switch all settings to «off».

If you would like to personalise certain settings and partly activate some, please wait until Windows has finished installing, and then change your settings.

Settings after Windows 10 installation (update)

Should you already have installed (updated) Windows 10 with its standard settings, you can subsequently adjust settings in Windows. You will find the relevant menu under *Start* >  *(Settings)* > *Privacy*.

General

To protect your device against definite identification based on an advertising ID allocated by Windows, switch the first option «off».

You should leave the second option «on». This way, you ensure that websites are displayed in the language set as the Windows system language where possible.

The third option serves for local improvement of Windows and be left switched «on». Windows can launch apps in frequent use by you more quickly this way.

Option	Our recommendation	OK
Allow apps to use the advertising ID to display advertisements of interest to you based on your use of apps (when deactivating this option, your ID is reset)	Off	☐

Option	Our recommendation	OK
Let websites provide locally relevant contents by accessing my language list	On	☐
Allow Windows to track apps launching to improve start-up and search results	On	☐
Show me suggested content in the Settings app	Off	☐

Speech, inking & typing

Windows and the Cortana voice assistant can analyse your voice and handwriting and improve personal recommendations that way. Since this allows Windows 10 to spy on your calendar, contact data and similar, you should switch this option off.

Diagnostics & feedback

You cannot completely stop Microsoft from collecting any data. You can choose whether you would like to transmit few or plenty of data. To transmit as few data as possible, please select: «Basic».

Option	Our recommendation	OK
Improve inking and typing	Off	☐
Individual user experience	Off	☐
Diagnostic data display	Off	☐

Activity history

Windows analyses which applications you have been working with, and offers a history of your activities.

If you use a Microsoft account and have cloud synchronisation activated, this will allow you to access the same timeline on several devices. If you don’t want this, you should switch it off.

Option	Our recommendation	OK
Let Windows collect my activities from this PC	Off	☐
Let Windows sync my activities from this PC to the cloud	Off	☐

Location

Location detection should be switched off. By clicking on «Clear», you can delete your location history stored so far.

Should you have a GPS receiver, you can enable or disable location detection for each of your installed apps individually.

Option	Our recommendation	OK
Location setting	Off	☐

Camera

Here you can stop every app automatically given access to your camera. Switch this option off.

Should you have a camera and would like to allow access to individual apps, you should do this for each app and enable or disable access for each one individually.

Option	Our recommendation	OK
Allow access to the camera on this device	Off	☐

Microphone

Here you can stop every app automatically given access to your microphone Switch this option off.

Should you have a microphone and would like to allow access to individual apps, you should do this for each app and enable or disable access for each one individually.

Option	Our recommendation	OK
Allow access to the microphone on this device	Off	☐

Notifications

You can basically enable or disable access to your notifications for all apps generally. If you don't want to generally stop all access, you can enable or disable access for each app individually. Access should only be granted to trustworthy apps.

Account info

Since this access is primarily required for personalised advertising, it is recommended to switch this option off.

Option	Our recommendation	OK
Allow access to all your account information on this device	Off	☐

Contacts

You can basically enable or disable access to your contacts for all apps generally. If you don't want to generally stop all access, you can enable or disable access for each app individually. Access should only be granted to trustworthy apps.

Calendar

You can basically enable or disable access to your calendar for all apps generally. If you don't want to generally stop all access, you can enable or disable access for each app individually. Access should only be granted to trustworthy apps.

Call history

You can basically enable or disable access to your call history for all apps generally. If you don't want to generally stop all access, you can enable or disable access to every app individually. Access should only be granted to trustworthy apps.

Email

You can basically enable or disable access to your e-mail by all apps generally. If you don't want to generally stop all access, you can enable or disable access to every app individually. Access should only be granted to trustworthy apps.

Tasks

You can basically enable or disable access to your tasks by all apps generally. If you don't want to generally stop all access, you can enable or disable access to every app individually. Access should only be granted to trustworthy apps.

Messaging

You can basically enable or disable access by all apps to your messages (SMS or MMS) generally. If you don't want to generally stop all access, you can enable or disable access to every app individually. Access should only be granted to trustworthy apps.

Radios

You can basically enable or disable access to your radios (Bluetooth, etc.) by all apps generally. If you don't want to generally stop all access, you can enable or disable access to every app individually. Access should only be granted to trustworthy apps.

Other devices

An automatic exchange of information, for instance inside a public Wi-Fi network, poses a serious security risk. You should therefore switch this option off.

Please note however that contactless payments using a smartphone (with Windows 10 mobile phones) are no longer possible this way.

Option	Our recommendation	OK
Let your apps automatically share and sync info with wireless devices that don't explicitly pair with your PC, tablet or phone	Off	☐

Background apps

Microsoft terms a program a «background app» if it always remains up-to-date, even if you are not actively using it. Withdrawing this right from an app can help you save power. Particularly with mobile devices, this will make for a longer battery life. However, these settings have nothing to do with data protection. You can set this option as required by you.

App diagnostics

As per their default settings, apps also transmit many diagnostic data to Microsoft. It is recommended to switch this option «off».

Option	Our recommendation	OK
Let apps access diagnostic info	Off	☐

Automatic file downloads

Has been deactivated as per your settings above.

Documents

You can enable or disable access to your document libraries by all apps overall. If you don't want to generally stop all access, you can enable or disable access by every app individually. Access should only be granted to trustworthy apps.

Images

You can enable or disable access to your image libraries by all apps overall. If you don't want to generally stop all access, you can enable or disable access by every app individually. Access should only be granted to trustworthy apps.

Videos

You can enable or disable access to your video libraries by all apps overall. If you don't want to generally stop all access, you can enable or disable access by every app individually. Access should only be granted to trustworthy apps.

File system

You can enable or disable access to all your files, including your documents, images, videos and local OneDrive files, overall. If you don't want to generally stop all access, you can enable or disable access by every app individually. Access should only be granted to trustworthy apps.

Data protection dashboard

To guarantee the transparency of all data collected, Microsoft offers a data protection dashboard which lists all information stored. You can also delete these details as long as you are logged in via a Microsoft account.

Your data protection dashboard is available via this link: https://account.microsoft.com/privacy