

04.09.2025

App permissions – How to stay in control of your data

Many apps are asking for more access permissions than strictly necessary for them to function. If you regularly check and restrict permissions, you not only protect your privacy, but also prevent unwanted background usage of your data.

No matter whether a photo filter, game or social media app are involved – many of them require access to data and functions on your smartphone. This is sensible if access is needed for technical reasons, for instance if a photo editing app needs to access your photo gallery or a navigation app requires your location data. Yet apps frequently also ask for more extensive permissions – for instance if a torch app would like to access your contacts. Such excessive permissions may present some risks.

This is what you can do:

Android

- **Adjust access rights at any time:** Under Settings (Security and privacy > Privacy > Permission manager) you can see which apps have what kind of permissions and can either activate or deactivate them there.
- **Limited permissions:** From Android 11 upwards, instead of allowing access all the time, you can set sensitive permissions (for instance to access your camera, microphone or location), to “Allow only while using the app” or “Ask every time” instead.
- **Remove permissions if app is unused:** Apps not used over a longer period of time automatically lose sensitive permissions, such as those to access your camera or contacts.

iOS (iPhone, iPad)

- **Selectively administer permissions:** Under Settings > Privacy & Security, select relevant categories such as camera, microphone or location services to see which apps have access, which you can then selectively deactivate.
- **Limited permissions:** You can set sensitive permissions, for instance to access your camera, microphone or location, to “Allow once” or “Allow while using the app” instead.
- **App Privacy Report:** This function will show you when and how apps are accessing information obtained via your camera or microphone or from your network activities.