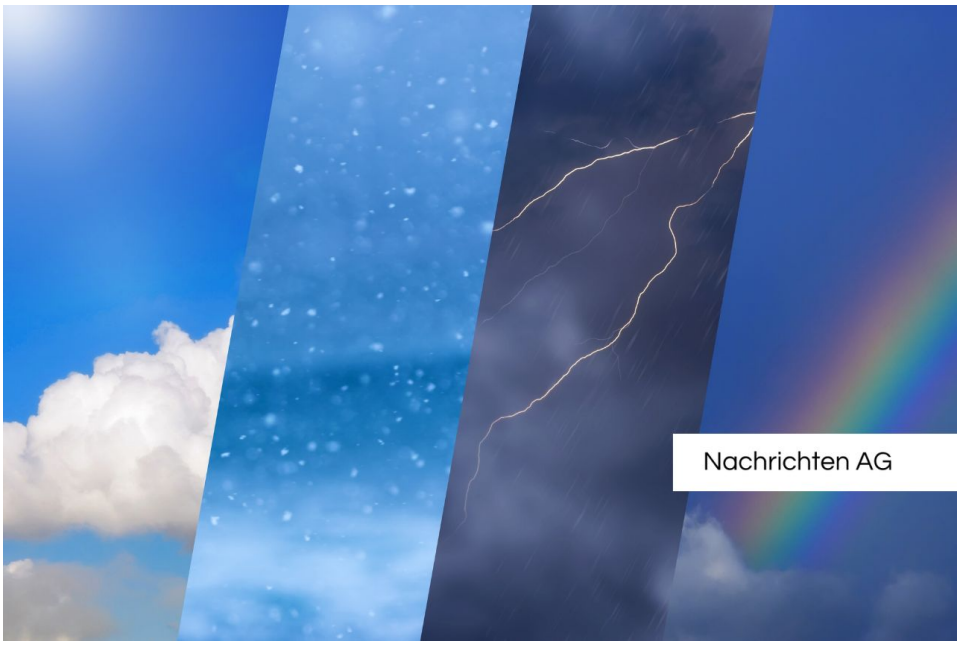
NACHRICHTEN AG

03. Juni 2025

Schütze deine Privatsphäre: Deaktiviere GPS, WLAN & Bluetooth!

Erfahren Sie, wie Sie GPS, WLAN und Bluetooth auf Smartphones deaktivieren, um Ihre Privatsphäre zu schützen und die Akkulaufzeit zu verbessern.



Keine Adresse oder kein Ort angegeben. - In einer Welt, in der Smartphones eine zentrale Rolle im Alltag spielen, ist der verantwortungsvolle Umgang mit Standortdaten von entscheidender Bedeutung. Eine aktuelle Empfehlung der Stiftung Warentest besagt, dass Nutzer ihre Funkverbindungen wie GPS, WLAN und Bluetooth nur bei Bedarf aktivieren sollten. Diese Maßnahme dient nicht nur dem Schutz der Privatsphäre, sondern kann auch dazu beitragen, die Akkulaufzeit zu verlängern. Bei niedrigem Akkustand kann das Abschalten nicht benötigter Funkverbindungen entscheidende Minuten Laufzeit gewinnen, was für viele Nutzer von großem Vorteil ist. Laut tz.de ist es zudem wichtig, die ȣStandortgenauigkeit verbessernȣ-Funktion zu deaktivieren, um zusätzliche

Datensammelvorgänge zu verhindern.

Ein weiteres Risiko besteht darin, dass ungenutztes Bluetooth ein potenzielles Sicherheitsrisiko darstellen kann. Schwachstellen in Bluetooth-Implementierungen könnten Angreifern Zugang zu Smartphones ermöglichen. Die Deaktivierung dieser Funkverbindungen auf Android-Geräten kann einfach über die Schnelleinstellungen erfolgen, während iPhone-Nutzer darauf achten sollten, dass eine dauerhafte Deaktivierung in den Einstellungen vorgenommen werden muss.

Standortdaten und ihre Auswirkungen

Die Erfassung von Standortdaten erfolgt durch verschiedene Technologien, darunter Mobilfunknetz, WLAN, Bluetooth und GPS. Diese Daten sind nicht nur für die Nutzung von Location Based Services (LBS) wie Routenberechnung oder ortsbezogenem Wetter wichtig, sie tragen auch zur Erstellung detaillierter Bewegungsprofile bei. Diese können zur Identifizierung von Personen führen und gelten nach der Datenschutz-Grundverordnung (DSGVO) als personenbezogene Daten. Laut datenschutzexperte.de sollten Nutzer daher standardmäßig alle Standortdaten auf ihren Smartphones deaktivieren.

Einige Apps sammeln selbst im Hintergrund Daten, was bedeutet, dass eine sorgfältige Auswahl und Überprüfung von Berechtigungen notwendig ist. Nutzer sollten nur jenen Apps Zugriff auf Standortdaten gewähren, die diese für ihren Betrieb zwingend benötigen. Anleitungen zur Deaktivierung dieser Funktionen sind sowohl für Android- als auch iPhone-Geräte verfügbar. Auf Android-Geräten kann dies über die Schnelleinstellungen geschehen, während iPhone-Nutzer die Einstellungen unter ȝDatenschutz > Ortungsdienstеȝ anpassen müssen.

Datenschutz und Risiken

Ein Augenmerk sollte auch auf das langfristige Speichern von Standortdaten gelegt werden. Laut dg-datenschutz.de führen solche Daten zu detaillierteren Bewegungsprofilen, die für gezielte Werbung genutzt werden können. Kontaktloses Bezahlen fügt dem Interessens-Profil der Nutzer zusätzliche Informationen hinzu, was den digitalen Fußabdruck weiter vergrößert. Algorithmen, die Muster in Bewegungen erkennen, können sogar zukünftige Aufenthaltsorte vorhersagen.

Zusammenfassend ist der Umgang mit Standortdaten eine kritische Thematik, die sowohl aus datenschutzrechtlicher Sicht als auch im Hinblick auf die persönliche Sicherheit von Bedeutung ist. Nutzer sollten sich bewusst sein, welche Daten sie preisgeben und entsprechende Vorkehrungen treffen, um ihre Privatsphäre zu schützen.

Details	
Ort	Keine Adresse oder kein Ort angegeben.
Quellen	• www.tz.de • www.datenschutzexperte.de • dg-datenschutz.de

Besuchen Sie uns auf: n-ag.net