

WIE KÖNNEN SIE SICH NOCH SCHÜTZEN?

Smartphones sind heutzutage leistungsfähige Computer. Daher sollten ähnliche **Sicherheitsvorkehrungen** wie bei PC oder Laptop beachtet werden. Je besser Ihr Gerät und Ihre Daten gesichert sind, desto schwerer haben es Datendiebe, sich Zugriff zu verschaffen. Wir haben für Sie wichtige Schutzmaßnahmen zusammengestellt:

Halten Sie das Betriebssystem und installierte Anwendungen durch regelmäßige, am besten **automatische Updates** auf dem aktuellen Stand. Auch **Virenschutz** und **Firewall** sind beim Smartphone zu empfehlen.

Schützen Sie Ihre Daten durch **komplexe Passwörter** (mindestens acht, besser zwölf Zeichen, Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen) und nutzen Sie **Verschlüsselungsmöglichkeiten**.

Sichern Sie insbesondere den Zugang zu **Banking-Apps** und **Apps mit Bezahlfunktion**. Reagieren Sie nicht auf Aufforderungen, PIN- oder TAN-Nummern offenzulegen. Vermeiden Sie das mobile TAN-Verfahren (mTAN, s. Glossar), wenn Sie das gleiche Gerät zum Online-Banking verwenden.

Aktivieren Sie die **Fernlöschfunktion** Ihres Smartphones. Löschen Sie Ihre Daten, bevor Sie das Smartphone zur Reparatur geben oder verkaufen.

Deaktivieren Sie **ungenutzte Funktionen** wie GPS, WLAN, Bluetooth oder NFC. Meiden Sie öffentlich zugängliche Internetzugänge wie **WLAN-Hotspots**, insbesondere bei vertraulichen Vorgängen.

IHR GUTES RECHT

Von Ihrem Anbieter können Sie **Auskunft** darüber verlangen, welche persönlichen Daten zu welchem Zweck gespeichert sind, an wen sie möglicherweise weitergegeben wurden und woher sie stammen. Falsche Daten sind auf Ihren Antrag hin zu berichtigen. Sollten Sie keine Einwilligung zur Datenspeicherung und -verwendung erteilt haben, können Sie die **Löschung** der Daten beantragen. Beachtet ein Anbieter Ihre Rechte nicht, wird er unter Umständen schadensersatzpflichtig. Außerdem haben Sie die Möglichkeit, der Verwendung Ihrer Daten zu Werbe- und Marktforschungszwecken zu **widersprechen**.

Mit einem einfachen Brief machen Sie Ihre Rechte gegenüber einem Anbieter geltend. Musterschreiben finden Sie z. B. auf der Seite der Verbraucherzentrale Rheinland-Pfalz www.verbraucherzentrale-rlp.de/musterbriefe/digitale-welt.

Sollte der Anbieter Ihre Rechte ignorieren, wenden Sie sich an die für den Sitz des Anbieters zuständige Datenschutzaufsichtsbehörde. Auch der Landesdatenschutzbeauftragte und die Verbraucherzentrale Rheinland-Pfalz helfen Ihnen gerne weiter.



GLOSSAR

Cookies

sind kleine Dateien, die der Browser beim Surfen im Internet auf Ihrem Endgerät speichert. Sie enthalten z. B. Informationen über besuchte Seiten und persönliche Einstellungen.

GPS (Global Positioning System)

ist ein globales Satellitennavigationssystem zur Positionsbestimmung.

mTAN (Mobile Transaktionsnummer)

ist ein zeitlich limitierter Zahlencode zur Autorisierung von Online-Bankgeschäften, der per SMS auf das Mobiltelefon des Kunden geschickt wird und auf der Webseite der Bank eingegeben werden muss.

NFC (Near Field Communication)

ist ein Funkstandard zur drahtlosen Datenübertragung zwischen zwei NFC-fähigen Geräten. Er wird zum Beispiel für kontaktloses Bezahlen mit dem Smartphone genutzt.

Tracking

ist eine technische Möglichkeit, um Besucherströme, -verhalten und -aktionen auf Webseiten zu verfolgen. Ziel ist es, Nutzungs- und Verhaltensprofile zur Optimierung von Online-Marketingmaßnahmen zu erstellen.

WLAN-Ortung

ermöglicht die Standortberechnung anhand von WLAN-Signalen, die ein Smartphone von Hotspots, öffentlichen oder privaten Netzwerken empfängt.

KONTAKT

Ministerium für Familie, Frauen, Kultur und Integration

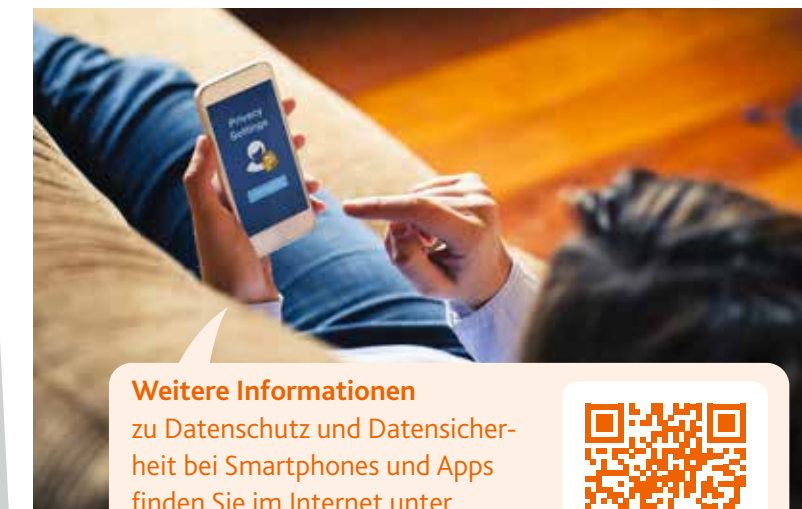
Kaiser-Friedrich-Straße 5a, 55116 Mainz
Telefon: +49 (0) 6131 16-0
poststelle@mffki.rlp.de | www.mffki.rlp.de

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

Hinterre Bleiche 34, 55116 Mainz
Telefon: +49 (0) 6131 208-2449
poststelle@datenschutz.rlp.de | www.datenschutz.rlp.de

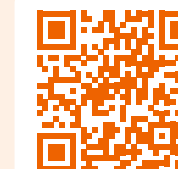
Verbraucherzentrale Rheinland-Pfalz e.V.

Seppel-Glückert-Passage 10, 55116 Mainz
Telefon: +49 (0) 6131 2848-0
info@vz-rlp.de | www.verbraucherzentrale-rlp.de



Weitere Informationen

zu Datenschutz und Datensicherheit bei Smartphones und Apps finden Sie im Internet unter
s.rlp.de/smartphones oder
youngdata.de.



DER SPION IN DER HOSENTASCHE

Datenschutz auf dem Smartphone



Impressum

Ministerium für Familie, Frauen, Kultur und Integration (Hrsg.)

Kaiser-Friedrich-Straße 5a, 55116 Mainz
© 06131 16-0 (zentraler Telefondienst), www.mffki.rlp.de

Redaktion

Patricia C. Krieger (Referat Reden und Öffentlichkeitsarbeit), Ingmar Bonmann (Referat Verbraucherschutz)

Design und Illustration: Sascha Jaeck

Bildnachweis Innenseite, v. l. n. r.:

© WavebreakMediaMicro, © Andrey Popov / fotolia.com

Außenseite, v. l. n. r.: © pictworks, © daviles / fotolia.com

Druck: Druckhaus Franz Seibert GmbH & Co. KG

Erscheinungstermin: Februar 2023

Diese Druckschrift wird im Rahmen der Öffentlichkeitsarbeit der Landesregierung Rheinland-Pfalz herausgegeben. Sie darf weder von Parteien noch Wahlbewerberinnen und -bewerbern oder Wahlhelferinnen und -helfern im Zeitraum von sechs Monaten vor einer Wahl zum Zweck der Wahlwerbung verwendet werden. Dies gilt für Kommunal-, Landtags-, Bundestags- und Europawahlen. Missbräuchlich ist während dieser Zeit insbesondere die Verteilung auf Wahlveranstaltungen, an Informationsständen der Parteien sowie das Einlegen, Aufdrucken und Aufkleben parteipolitischer Informationen oder Werbemittel. Untersagt ist gleichfalls die Weitergabe an Dritte zum Zweck der Wahlwerbung. Auch ohne zeitlichen Bezug zu einer bevorstehenden Wahl darf die Druckschrift nicht in einer Weise verwendet werden, die als Parteinahme der Landesregierung zugunsten einzelner politischer Gruppen verstanden werden könnte. Den Parteien ist es gestattet, die Druckschrift zur Unterrichtung ihrer eigenen Mitglieder zu verwenden.

VORWORT



Katharina Binz

Liebe Leserinnen und Leser, wer möchte heute noch auf sein Smartphone oder Tablet verzichten? Haben wir doch viele nützliche Apps, die uns den Alltag erleichtern oder auch einfach nur Spaß machen. Die Digitalisierung unseres Alltags ist eine Erfolgs-

story – aber nicht nur! Viele Apps und digitale Dienste sowie auch die Geräte selbst sammeln eine Menge Daten – manchmal offen und manchmal auch sehr versteckt. Das betrifft nicht nur Sie persönlich als Nutzerin oder Nutzer, sondern geht darüber hinaus, indem Sie zum Beispiel Ihre Kontakte freigeben oder Fotos von Familie und Freunden teilen.

Über das sogenannte „Big Data“ (große Datenmengen) lassen sich die verschiedensten Analysen durchführen und sehr präzise Aussagen über Sie persönlich treffen. Dieses Datensammeln müssen Sie jedoch nicht dulden. Denn Ihre Rechte werden in ganz Europa in vielfältiger Weise geschützt, wie beispielsweise durch die Datenschutzgrundverordnung oder spezielle Regelungen zum Datenschutz.

Was aber können Sie tun, wenn Sie digital dabei sein wollen, doch den Überblick über Ihre Daten behalten möchten? Es gibt einfache Wege, die Ihnen helfen, Ihre digitalen Helfer vor dem unerwünschten Zugriff Dritter zu schützen. Und natürlich gibt es Stellen, bei denen Sie sich gezielt informieren und bei Bedarf auch Hilfe holen können. Nehmen Sie sich deshalb ein paar Minuten Zeit für diesen Flyer.

Ich wünsche Ihnen eine informative Lektüre.

Ministerin für Familie, Frauen, Kultur und Integration in Rheinland-Pfalz

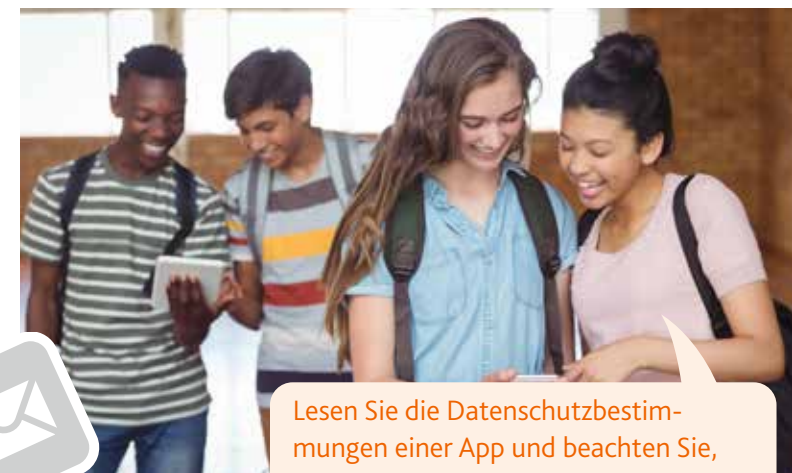
WAS VERRÄT IHR SMARTPHONE ÜBER SIE?

Smartphones speichern eine Vielzahl **persönlicher Daten**, von denen Sie viele selber eingeben. Das gilt zum Beispiel für Kontakte, Fotos und Textnachrichten, aber auch für Bankverbindungen oder Passwörter. Andere Daten, etwa die von Ihnen **besuchten Internetseiten**, werden ohne Ihr Zutun erfasst. Darüber hinaus kann Ihr Smartphone über die **GPS-Daten** ebenso wie über die **Bluetooth-** oder **WLAN-Ortung** verraten, wo Sie sich gerade aufhalten – vorausgesetzt, Sie haben die jeweiligen Funktionen aktiviert.



In der Standardeinstellung sind die Geräte mitunter sehr mitteilbar. Überprüfen Sie daher bereits bei Inbetriebnahme die Voreinstellungen auf ungewollte Datenübertragungen.

Überlegen Sie, welche Daten Sie Ihrem Smartphone anvertrauen. Bedenken Sie, dass es nicht nur um Ihre, sondern auch um die Ihrer Familie, Freunde oder Geschäftspartner geht.



Lesen Sie die Datenschutzbestimmungen einer App und beachten Sie, dass diese sich ebenso wie die Einstellungsoptionen jederzeit ändern können. Schränken Sie die Rechte einer App so weit wie möglich ein. Prüfen Sie datenschutzfreundlichere Alternativen, selbst wenn sie kostenpflichtig sein mögen.

Vor allem **Apps** können Ihre Privatsphäre ausspionieren, indem sie gespeicherte Daten Ihres Smartphones auslesen und weiterverwenden. Ein solcher Zugriff ist nur mit Ihrer **Einwilligung** zulässig. Nicht immer wird Nutzerinnen und Nutzern bewusst, welche umfangreichen Rechte sie den Betreibern und möglichen Drittanbietern manchmal einräumen. Kostenlose Apps sind in der Regel besonders neugierig.

WER HAT INTERESSE AN IHREN DATEN?

Gerätehersteller, Provider oder Betreiber von Apps profitieren davon, dass Sie mit dem Smartphone online sind. Denn aus Ihren Daten und den Spuren, die Sie im Netz hinterlassen, können sogenannte **Nutzerprofile** gebildet werden. Ein Nutzerprofil beschreibt Verhaltensweisen oder Gemeinsamkeiten von Zielgruppen und ist daher bares Geld wert.

Mit den Informationen kann **Werbung** gezielt auf Ihre Bedürfnisse zugeschnitten werden. Das kann auch dazu führen, dass Sie bestimmte Angebote nicht mehr erhalten, wenn Sie für ein Unternehmen als Kundin oder Kunde unattraktiv geworden sind. Auch im Online-Shop angezeigte Preise können auf eine **Profilbildung** zurückgehen.

Der Profilbildung können Sie entgegenwirken, indem Sie zum Beispiel Tracking im Browser deaktivieren, die Browserdaten regelmäßig löschen sowie Cookies und die Standorterfassung nur bei Bedarf zulassen.

Bei manchen Apps können Sie interessenbezogene Werbung ablehnen.



Auch unseriöse Anbieter haben erkannt, dass das Smartphone der perfekte Spion in der Hosentasche ist. Sie locken zum Beispiel mit Gratis-Apps für Spiele, Bilder oder andere Angebote. Darin kann **Schadsoftware** verpackt sein, die Daten heimlich sammelt oder ungefragt weitersendet. Meistens ist nicht nachvollziehbar, was mit den Daten geschieht und wer sie erhält.

Nutzen Sie nur Apps aus vertrauenswürdigen Quellen, d. h. den Softwareportalen der Geräte- bzw. Betriebssystemhersteller. Nehmen Sie keine Eingriffe am Betriebssystem vor.

Löschen Sie Nachrichten aus unbekanntem Quellen, ohne sie zu öffnen, da auch hier Schadsoftware enthalten sein kann.