Smartphones speichern eine Vielzahl persönlicher Nutzerdaten: Manche Daten wie zum Beispiel Kontakte, Fotos oder Textnachrichten, aber auch Bankverbindungen oder Passwörter speisen Sie als Benutzer selbst ein. Andere Daten wiederum werden ohne Ihr Zutun erfasst: So wird beim Surfen im Internet – wie beim PC oder Laptop – auch gespeichert, welche Internetseiten Sie besuchen. Darüber hinaus kann Ihr Smartphone über die GPS-Daten verraten, wo Sie sich gerade aufhalten. Hierzu ist allerdings Ihre Zustimmung erforderlich. Insgesamt steht fest: „Smartphones sind klein, aber oho."

Daneben kann die Verwendung von Apps Datenschutzprobleme mit sich bringen. Viele Apps senden die Gerätenummer (sog. UDID) an den Server des Anbieters und machen Ihr Smartphone damit eindeutig identifizierbar. Nicht immer ist die hierzu notwendige Nutzereinwilligung transparent gestaltet. Zudem greifen Anwendungen teilweise ohne Wissen der Nutzer auf das Gerät zu und lesen zum Beispiel Ihr Adressbuch, Ihre E-Mails, SMS oder den Browserverlauf aus. Ein Zugriff ohne Einwilligung ist rechtlich unzulässig.

Gefahren können auch außerhalb Ihres Smartphones lauern: Wenn Sie beispielsweise Ihr WLAN oder Bluetooth unkontrolliert aktiviert lassen, halten Sie die Tür für unbemerkte Zugriffe von außen offen. Auch an öffentlich zugänglichen Internetzugängen sollten Sie vorsichtig sein. Das Gerät ist dort angreifbar und es besteht die Möglichkeit, dass Dritte Ihre Daten ausspähen können.

Unser gleichnamiges Internetangebot informiert Sie aktuell und verständlich über Ihre Rechte und die sichere Nutzung Ihres Smartphones.

www.mjv.rlp.de/smartphones

KONTAKT

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz
Hintere Bleiche 34, 55116 Mainz
Telefon: +49 (0) 6131 208-2449
poststelle@datenschutz.rlp.de
www.datenschutz.rlp.de

Ministerium der Justiz und für Verbraucherschutz
Ernst-Ludwig-Str. 3, 55116 Mainz
Telefon: +49 (0) 6131 16- 4800
poststelle@mjv.rlp.de | www.mjv.rlp.de

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

Stand: August 2012 | **Bildnachweis:** Titelmontage Fotolia © Thomas Hammer und kazoka303030

verbraucherzentrale Rheinland-Pfalz

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz

RheinlandPfalz
MINISTERIUM DER JUSTIZ UND FÜR VERBRAUCHERSCHUTZ

SMARTPHONES UND APPS

Spione in der Hosentasche

WAS VERRÄT IHR SMARTPHONE ÜBER SIE?

Ob mailen, surfen oder navigieren: Smartphones sind nicht nur Mobiltelefone, sondern vielmehr „transportable Computer", die über verschiedene Datenschnittstellen, GPS-Ortung und einen mobilen Internetzugang verfügen. Entsprechend breit ist das Spektrum ihrer Nutzungsmöglichkeiten: Die kleinen Multitalente können zum Beispiel Termine, Dokumente und Adressen verwalten und als mobiles Büro fungieren. Vor allem lassen sie sich mit Zusatzprogrammen, den sogenannten Apps (von englisch: application / Anwendung), um beliebige Funktionen erweitern.

Apps können unter anderem die günstigste nächstgelegene Tankstelle anzeigen, das Wetter vorhersagen, die Kommunikation mit Freunden oder aber Überweisungen ermöglichen.

„Verbraucherinnen und Verbraucher müssen über ihre Daten selbst bestimmen können. Dazu brauchen sie transparente Informationen, wer welche Daten zu welchem Zweck erhebt, und Sicherheit durch technische Voreinstellungen.
Mit diesem Flyer möchten wir Ihnen Wege aufzeigen, wie Sie sich und Ihr Smartphone vor ungewollten Datenübertragungen schützen können."

Jochen Hartloff,
Minister der Justiz und für Verbraucherschutz
Rheinland-Pfalz

WER HAT INTERESSE AN IHREN DATEN?

Ihr Smartphone gefällt nicht nur Ihnen – auch Gerätehersteller, Provider oder Betreiber von Apps können davon profitieren, dass Sie mit dem Handy online sind. Denn so können sie Informationen erhalten, die sie sonst nie erfahren würden. Oft sind diese Daten für die Nutzung der Geräte oder Anwendungen nicht erforderlich, wohl aber für die Bildung von sogenannten Nutzerprofilen. Ein Nutzerprofil beschreibt Verhaltensweisen oder Gemeinsamkeiten von Zielgruppen.
Es kann auch auf weiteren Daten basieren, die zum Beispiel aus sozialen Netzwerken oder Online-Shops gewonnen werden können.

Ein solches Nutzerprofil ist bares Geld wert. Denn mit den Informationen kann kommerzielle Werbung gezielt auf Ihre Bedürfnisse zugeschnitten werden. Profilbildung kann auch bewirken, dass Sie bestimmte Angebote in Zukunft nicht mehr erhalten, da Sie für ein Unternehmen als Kunde dauerhaft unattraktiv geworden sind.

Das Smartphone ist also „der perfekte Spion in der Hosentasche". Auch unseriöse Anbieter haben dieses Potenzial erkannt und locken mit Gratis-Apps für Spiele, Bilder oder anderen Angeboten. Mit den Apps kommt aber nicht nur die erwartete Anwendung auf das Gerät. Im Programm kann auch Schadsoftware verpackt sein, die Daten heimlich sammelt und ungefragt weitersendet. Viele dieser Gratis-Programme können nur genutzt werden, sofern Sie bei der Installation in die Datenweitergabe einwilligen.

Wägen Sie daher Nutzen und Risiken ab. Jeder muss selbst entscheiden, ob sich für den Bezug zum Beispiel von Spielen, Scherz- oder Auskunftsprogrammen eine entsprechende Einwilligung wirklich lohnt. Schadsoftware lauert vor allem außerhalb der offiziellen Portale für Apps.

Meistens ist nicht nachvollziehbar, was mit den Daten geschieht und an wen sie weitergeleitet werden. Damit besteht die Gefahr, dass Ihre Nutzungsdaten unter Missachtung der Privatsphäre aus wirtschaftlichen Interessen als Ware gehandelt werden. Die Anbieter der Apps stammen zudem häufig aus dem nicht-europäischen Ausland, wohin dann auch die Daten fließen. Oft fehlen hierfür die entsprechende Rechtsgrundlage und die bei uns vorhandene Möglichkeit, Kontrolle und die eigenen Rechte auszuüben. Außerhalb von Europa sind das deutsche und europäische Datenschutzrecht nicht anwendbar.

„Das Smartphone sammelt vielfältige Daten über uns und unsere Kontakte. Wer das nicht will, muss die komplizierten Einstellungen des Telefons immer wieder anpassen. Nur so kann man verhindern, dass persönliche Profile erstellt werden, deren Auswirkungen Verbraucherinnen und Verbraucher derzeit noch nicht abschätzen können."

Ulrike von der Lühe,
Vorstand der Verbraucherzentrale Rheinland-Pfalz

WAS KÖNNEN SIE ZU IHREM SCHUTZ TUN?

Für manche Daten können Sie über entsprechende Einstellungen festlegen, ob Ihr Smartphone diese an den Hersteller des Gerätes oder eine App rückmeldet. Da die Geräte in der Standardeinstellung üblicherweise „sehr redselig" sind, sollten Sie Ihr Smartphone gleich bei der Inbetriebnahme dahingehend kontrollieren.

Bei der Nutzung von Apps sollten Sie Folgendes beachten:

- Verwenden Sie nur Apps aus sicheren Quellen, also den Softwareportalen der Geräte- bzw. Betriebssystemhersteller.
- Machen Sie sich mit den besonderen Datenschutzbestimmungen einer App vertraut. Beachten Sie, dass diese sich jederzeit ändern können.
- Nutzen Sie die Datenschutzeinstellungen, um ungewollte Datenübertragungen einzuschränken; Bluetooth, GPS und WLAN sollten nur aktiviert sein, wenn sie benötigt werden.
- Achten Sie darauf, welche Daten Sie auf Ihrem Smartphone gespeichert und abrufbar haben.
- Schützen Sie Ihre Daten durch Verschlüsselung, Passwort und ggf. die Löschfunktion nach Verlust.
- Löschen Sie Ihre Daten, bevor Sie das Smartphone zur Reparatur geben oder verkaufen.
- Virenschutz und Firewall sind beim Smartphone unbedingt zu empfehlen – auch wenn ihr Schutz nicht dem beim heimischen PC entspricht.
- Führen Sie Sicherheitsupdates durch und aktualisieren Sie regelmäßig die Firmware, also das Betriebssystem.

Sofern Sie wissen, wer Ihre Daten verwaltet, können Sie sich an diesen Anbieter wenden und Auskunft über die gespeicherten Daten fordern.

Lassen Sie sich mitteilen,

- worin Sie eingewilligt haben sollen; prüfen Sie gegebenenfalls einen Widerruf Ihrer Einwilligung und verlangen Sie die Löschung der Daten – vor allem wenn Sie nicht eingewilligt haben. Falsche Daten sind auf Ihren Antrag hin zu berichtigen.
- welche Daten über Sie gesammelt wurden, zu welchem Zweck und was damit passiert ist. Lassen Sie sich Dritte nennen, an die Ihre Daten möglicherweise weitergegeben wurden.

Achtet der Anbieter Ihre Rechte nicht, kann er sich schadensersatzpflichtig machen. Mit einem einfachen Brief können Sie Ihre Rechte gegenüber dem Anbieter geltend machen. Sollte der Anbieter Ihre Rechte ignorieren, wenden Sie sich an die für den Sitz des Anbieters zuständige Datenschutzaufsichtsbehörde – dort hilft man Ihnen weiter.

„Nutzerinnen und Nutzer müssen selbst entscheiden können, ob und wer ihre Daten erhält – und nicht Dritte über das Smartphone. Wenn die Hersteller und Betreiber dies nicht von sich aus gewährleisten, dann ist der Gesetzgeber gefordert."

Edgar Wagner,
Landesbeauftragter für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz