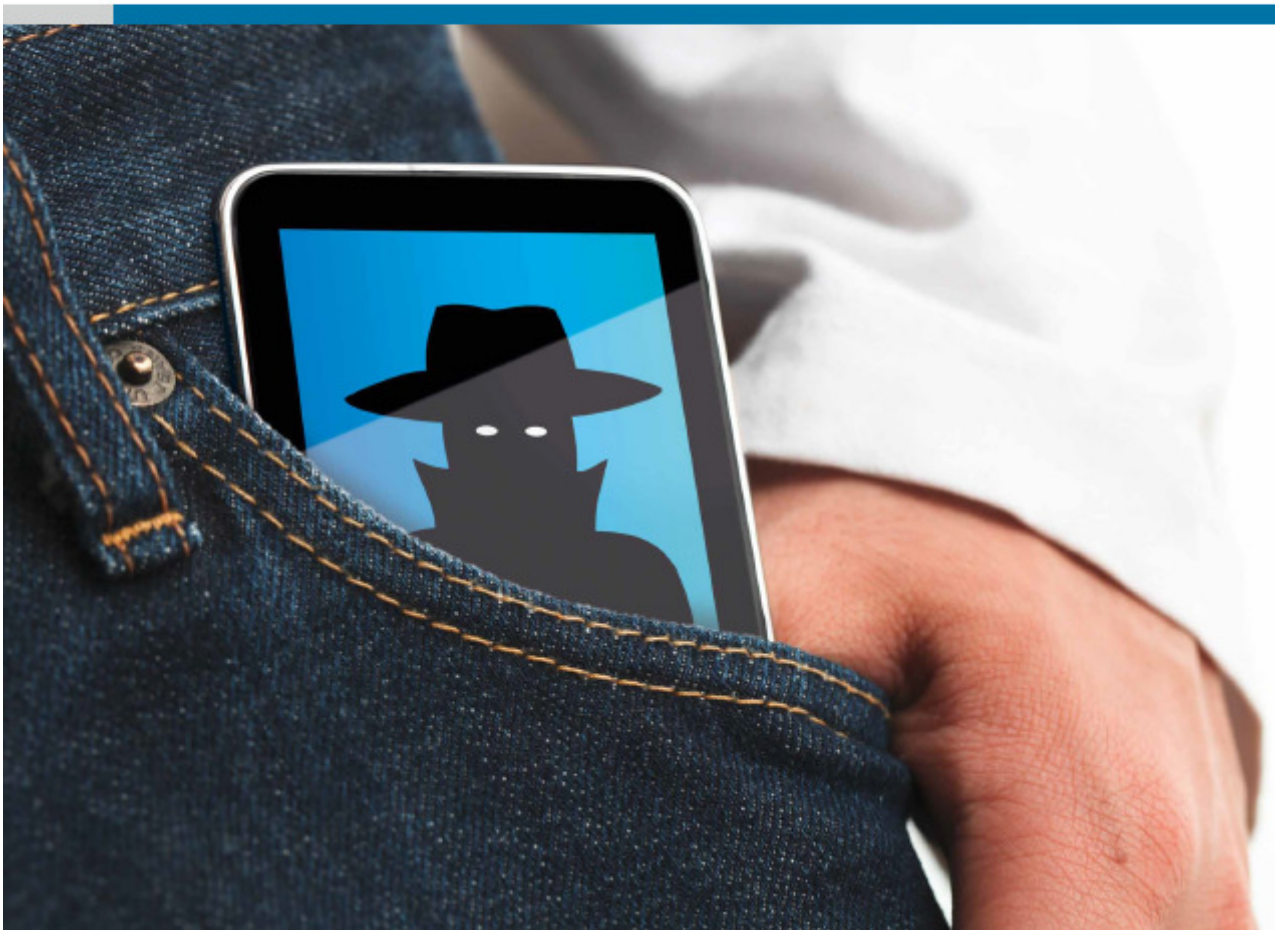
RheinlandPfalz
MINISTERIUM DER JUSTIZ UND FÜR VERBRAUCHERSCHUTZ

verbraucherzentrale
Rheinland-Pfalz

Der Landesbeauftragte
für den Datenschutz und die
Informationsfreiheit Rheinland-Pfalz

SMARTPHONES UND APPS

Spione in der Hosentasche



Hinweise zu den Datenschutzeinstellungen von Smartphones mit den Betriebssystemen Android und iOS

Inhalt **Seite**

A. Betriebssystem Android (Version 3.2)

1. Funknetz (WLAN) aktivieren/deaktivieren 4

2. Standortdaten (GPS) aktivieren/deaktivieren 4

3. Standortdaten für Google-Suche zulassen/untersagen 5

4. Speicherung von Sicherungsdaten bei Google zulassen/verweigern 5

5. Nahfunk (Bluetooth) aktivieren/deaktivieren 6

6. Bildschirmsperre / Passwort zur Freischaltung des Geräts festlegen 6

7. Passwort für die Freischaltung der SIM-Karte festlegen 7

8. Geräteverschlüsselung einstellen 8

9. Datenschutzeinstellungen für den eingebauten Android-Browser 9

A. Betriebssystem iOS (Version 5.1.1/6.1.3)

1. Ortungsdienste aktivieren/deaktivieren 12

2. Ortungsdienste für einzelne Programme zulassen/verbieten 12

3. Funknetz (WLAN) aktivieren/deaktivieren, Persönliche Hotspot-Funktion aktivieren/deaktivieren 13

4. Nahfunk (Bluetooth(aktivieren/deaktivieren 14

5. Smartphone mit Code-Sperre absichern 15

6. iCloud-Backup ausschalten 15

7. SIM-Karten PIN aktivieren 16

8. Datenschutzeinstellungen für den Browser „Safari“ 17

9. Allgemeine Datenschutzeinstellungen bei iOS 6.x 19

10. Deaktivieren der Tracking-Möglichkeit durch Werbeanbieter 20

Hinweis

Das Betriebssystem Android kommt in unterschiedlichen Versionen (Android 2.x, 3.x, 4.x) zum Einsatz, die zudem häufig von den Herstellern auf ihre Geräte angepasst wurden. Weiterhin stehen manche Einstellungsmöglichkeiten auf Tablet-Geräten, nicht jedoch auf Mobiltelefonen zur Verfügung. Möglicherweise unterscheiden sich daher die Einstellungsmöglichkeiten Ihres Geräts von den in dieser Übersicht genannten.

Die nachfolgenden Android-Beispiele beziehen sich auf die zum Stand der Veröffentlichung verbreitet eingesetzte Android Version 3.2 (Honeycomb). Unter der Version Android 4.0.x stehen die weitgehend gleichen Einstellungsmöglichkeiten unter z.T. jedoch geänderten Menübezeichnungen zur Verfügung (Drahtlos & Netzwerke (A.1, A.5), Standortdienste (A.2, A.3), Sicherheit (A.6), Sichern und Zurücksetzen (A.4)).

Apple iOS ist ebenfall in unterschiedlichen Versionen im Einsatz, wenngleich auch ältere Geräte mit aktuellen Betriebssystemversionen betrieben werden können. Die Beispiele beziehen sich auf die Version iOS 5.1.x. Auch hier können sich gegenüber Vorversionen Abweichungen ergeben.

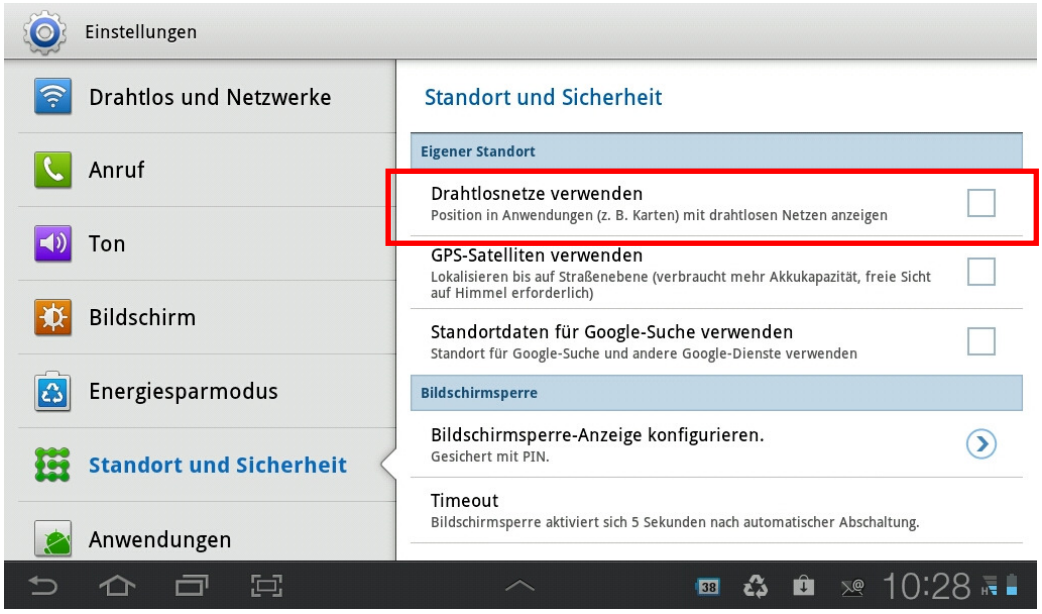
Stand: Mai 2013

A. Betriebssystem Android (Version 3.2)

1. Funknetz (WLAN) aktivieren/deaktivieren

Die WLAN-Funktionalität sollte erst dann aktiviert werden, wenn Sie benötigt wird, um eine ungewollte Preisgabe des Aufenthaltsorts zu vermeiden und Angriffsflächen zu reduzieren.

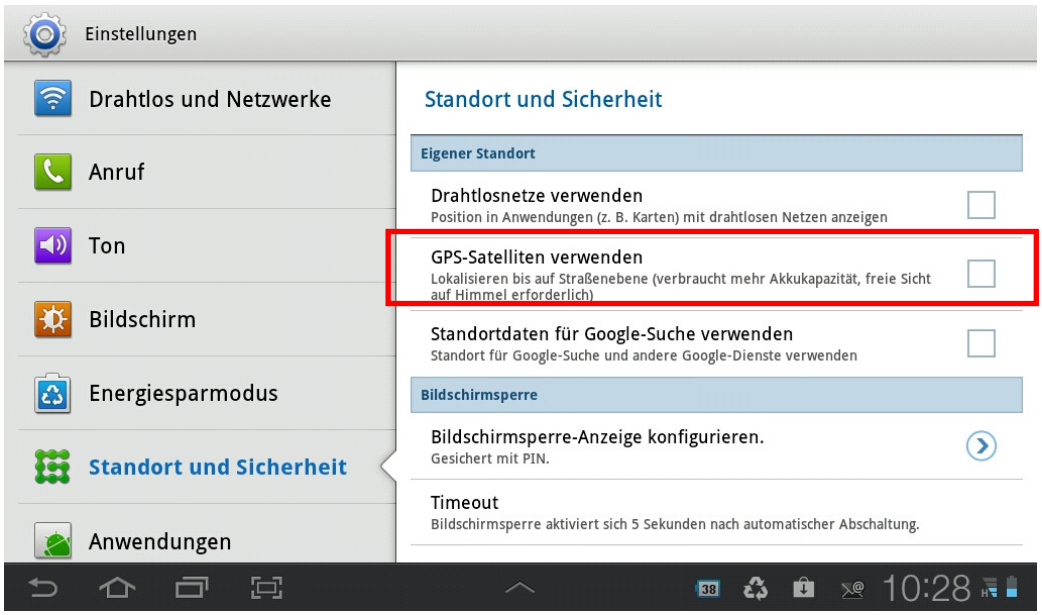
Einstellungen – Standort und Sicherheit



2. Standortdaten (GPS) aktivieren/deaktivieren

Die GPS-Funktionalität sollte erst dann aktiviert werden, wenn Sie benötigt wird, um eine ungewollte Preisgabe des Standorts zu vermeiden.

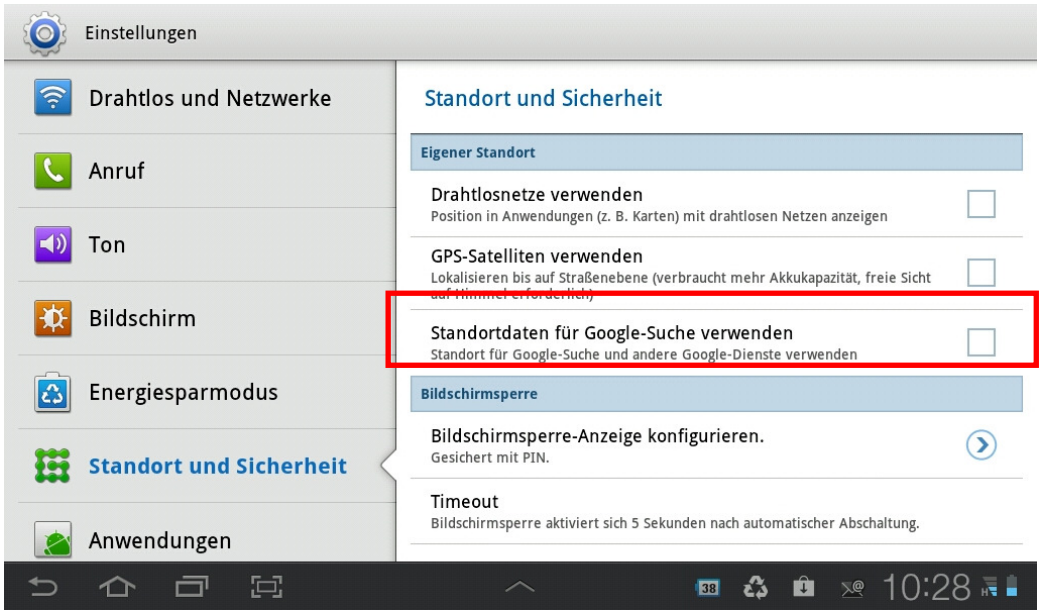
Einstellungen – Standort und Sicherheit



3. Verwendung von Standortdaten für die Google-Suche zulassen/verweigern

Wenn sie nicht benötigt wird, sollte die Verwendung der Standortdaten bei der Google Suche deaktiviert werden, um eine ungewollte Preisgabe des Aufenthaltsorts zu vermeiden

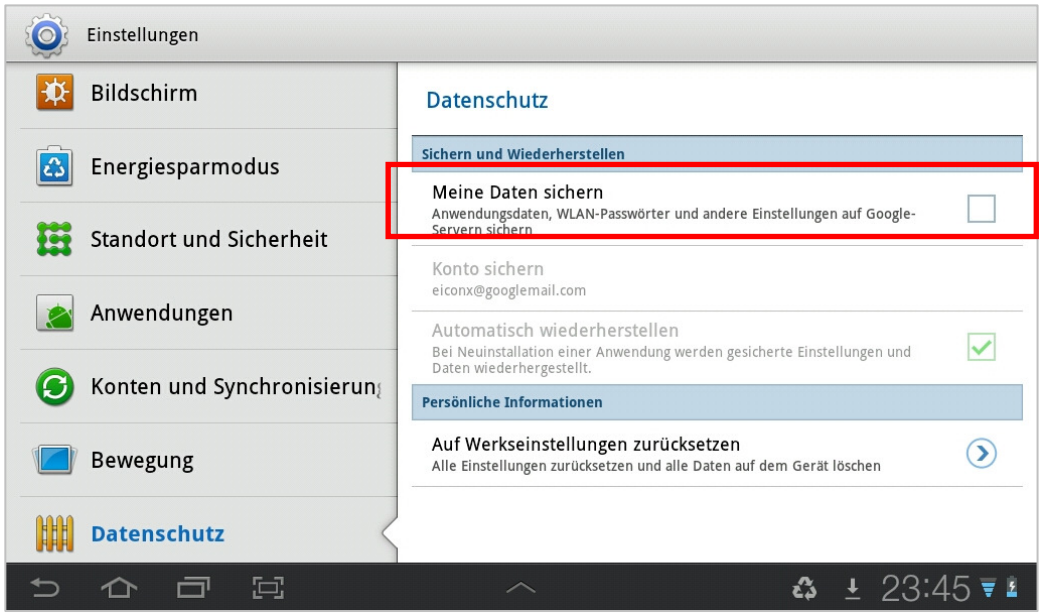
Einstellungen – Standort und Sicherheit



4. Speicherung von Sicherungsdaten bei Google zulassen/verweigern

Bei der Nutzung der Backup-Funktion von Google werden die Inhalte des Smartphones auf den Servern von Google gespeichert. Wenn man dies nicht möchte, sollte die Funktion deaktivert werden.

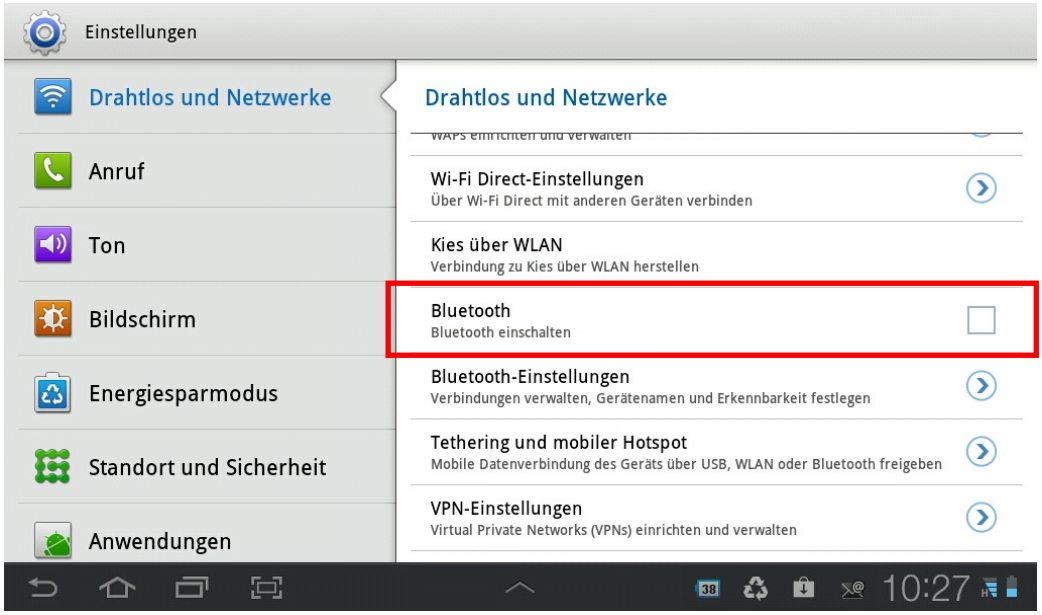
Einstellungen – Datenschutz



5. Nahfunk (Bluetooth) aktivieren/deaktivieren

Bei aktiverter Bluetooth-Funktion ist das Smartphone für andere Geräte in Ihrem Umfeld sichtbar und es können ggf. ungewollte Zugriffe erfolgen. Die Funktion sollte daher nur bei Bedarf aktiviert werden.

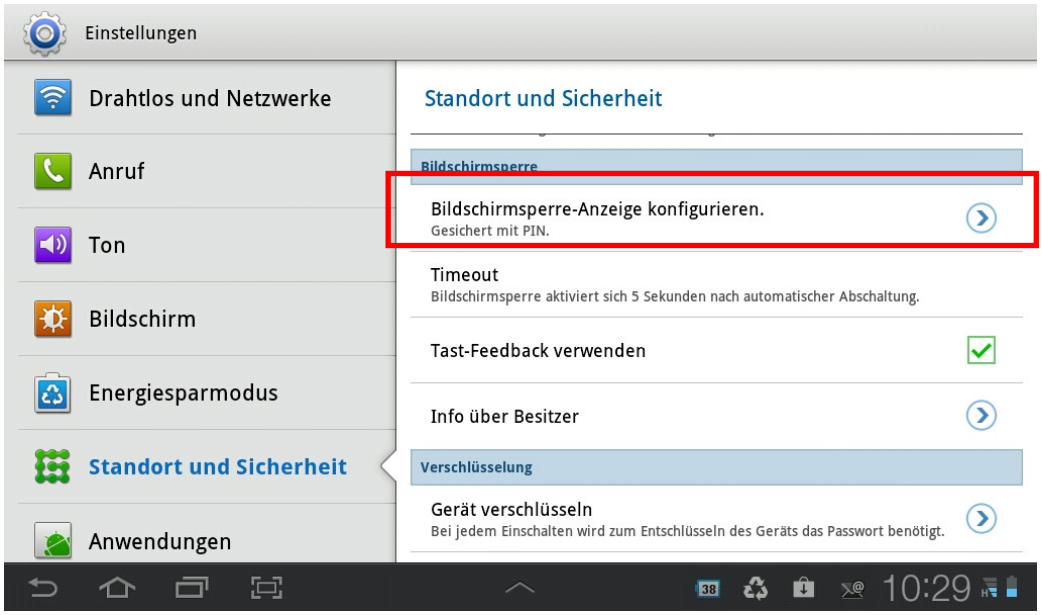
Einstellungen – Drahtlos und Netzwerke



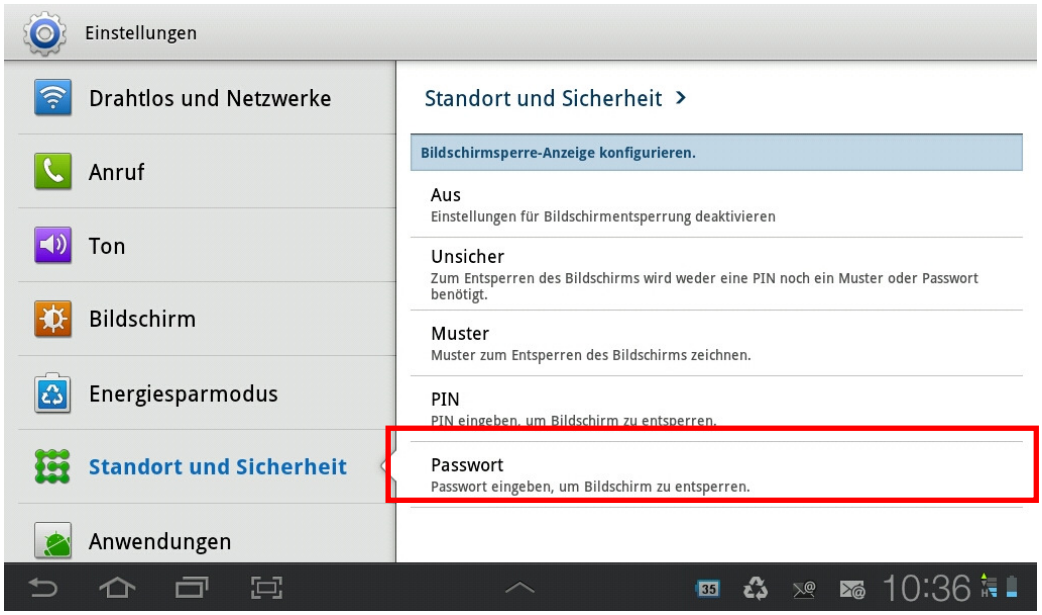
4. Bildschirmsperre / Passwort zur Freischaltung des Geräts festlegen

Um das Gerät vor einer unbefugten Nutzung zu schützen sollte das Smartphone mit einem Entsperrmuster, einer PIN oder einem Passwort geschützt werden.

Einstellungen – Standort und Sicherheit



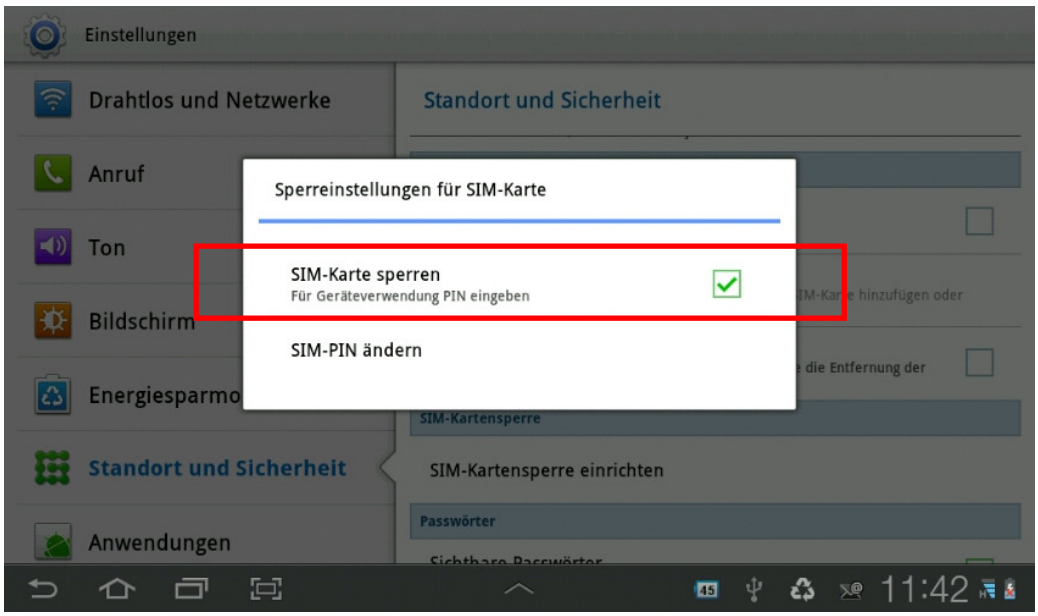
Einstellungen – Standort und Sicherheit – Bildschirmsperre-Anzeige konfigurieren



5. Passwort für die Freischaltung der SIM-Karte festlegen

Um die unbefugte Nutzung der Mobilfunkdienste des Smartphones zu nutzen, sollte die SIM-Karte mit einer PIN geschützt werden.

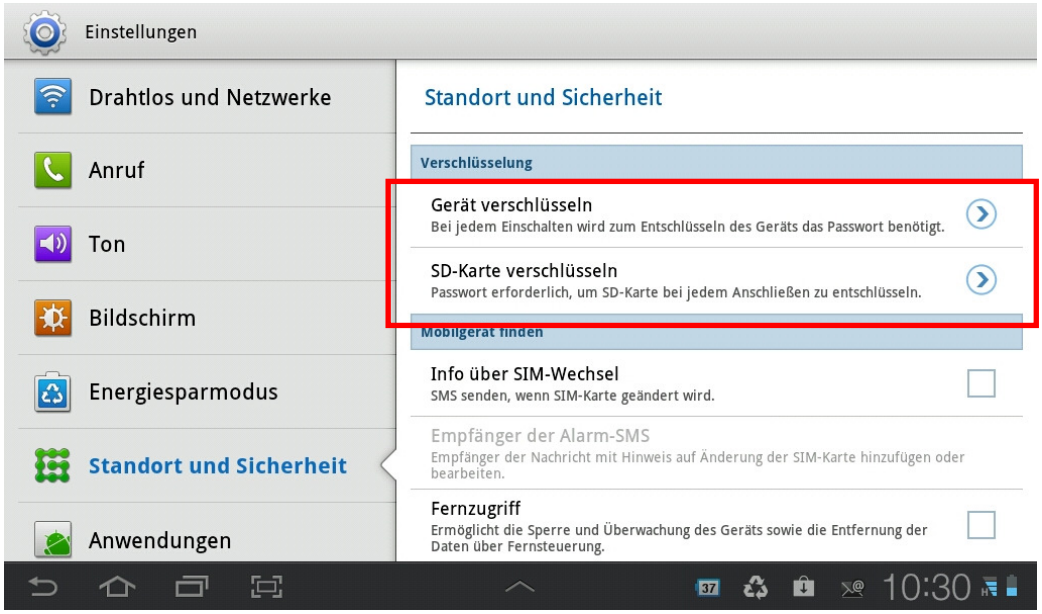
Einstellungen – Standort und Sicherheit – SIM-Kartensperre einrichten



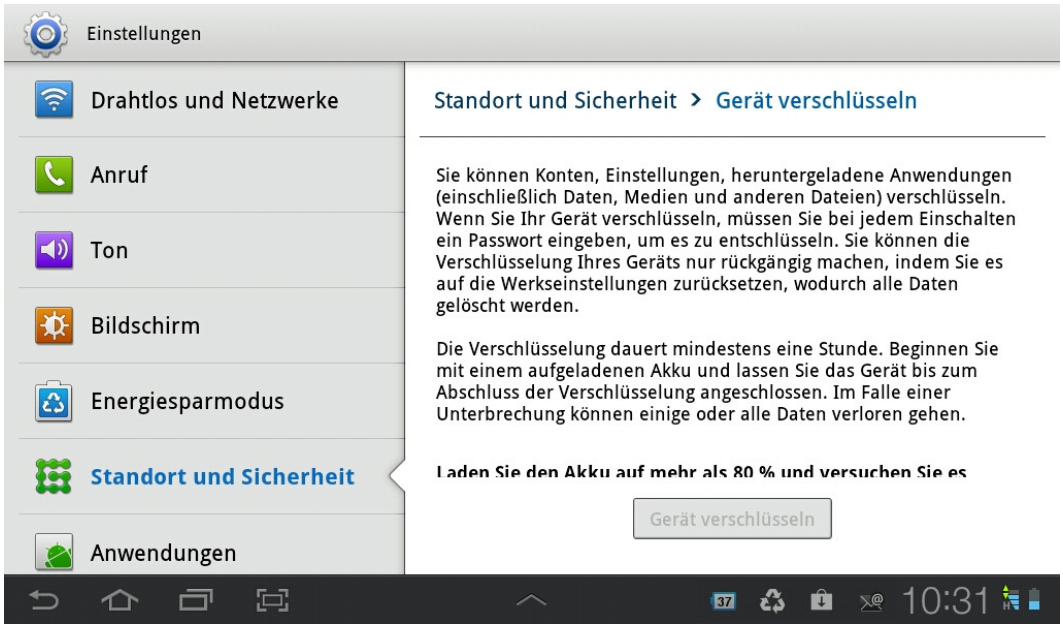
6. Geräteverschlüsselung einstellen

Um die Kenntnisnahme bei Verlust oder Diebstahl zu vermeiden, sollte die verschlüsselte Speicherung der Daten auf dem Smartphone aktiviert werden.

Einstellungen – Standort und Sicherheit



Einstellungen – Standort und Sicherheit – Gerät verschlüsseln

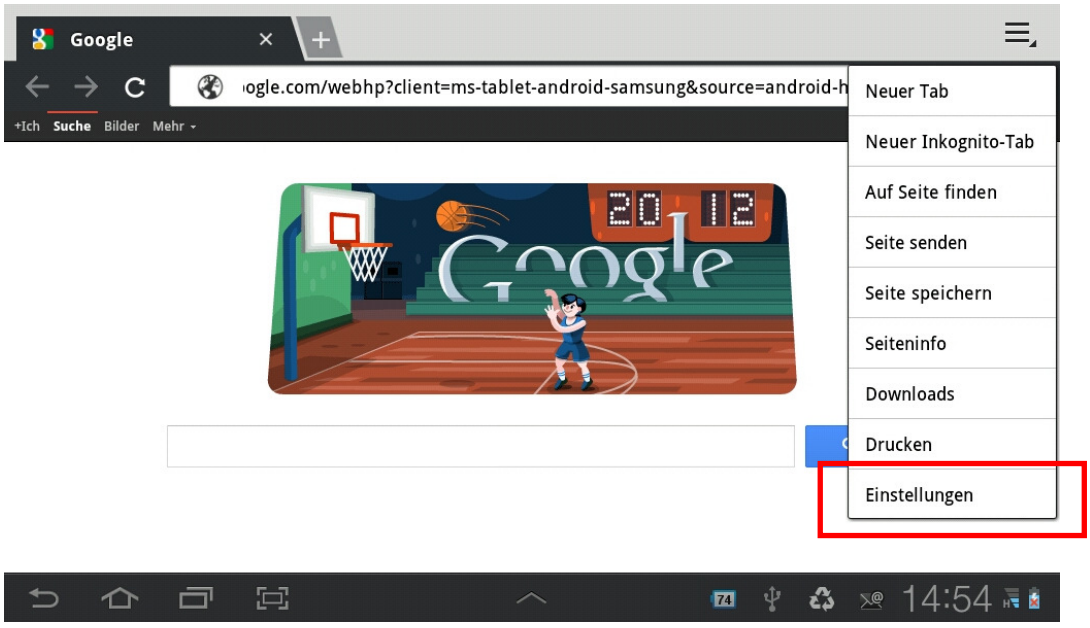


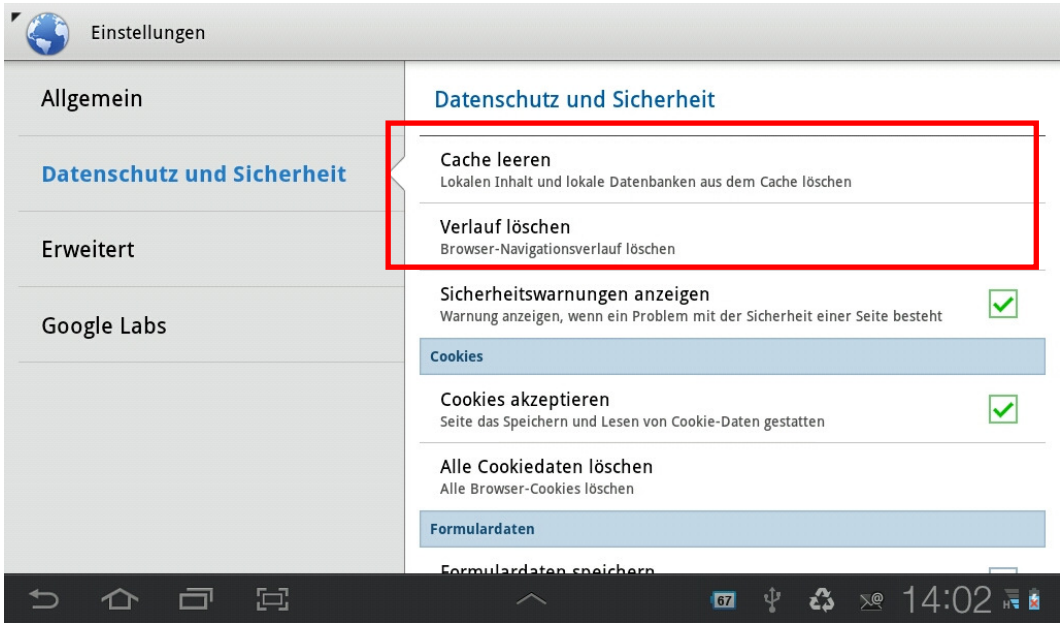
7. Datenschutzeinstellungen für den eingebauten Android-Browser

a) Browser-Cache und -Verlaufsanzeige, Cookies

Um die Datenspuren des Smartphone-Browsers zu reduzieren bzw. zu löschen, sollten in regelmäßigen Abständen Browser-Speicher (Cache) und Browser-Verlauf gelöscht werden.

In der Browseranwendung: Einstellungen – Datenschutz und Sicherheit

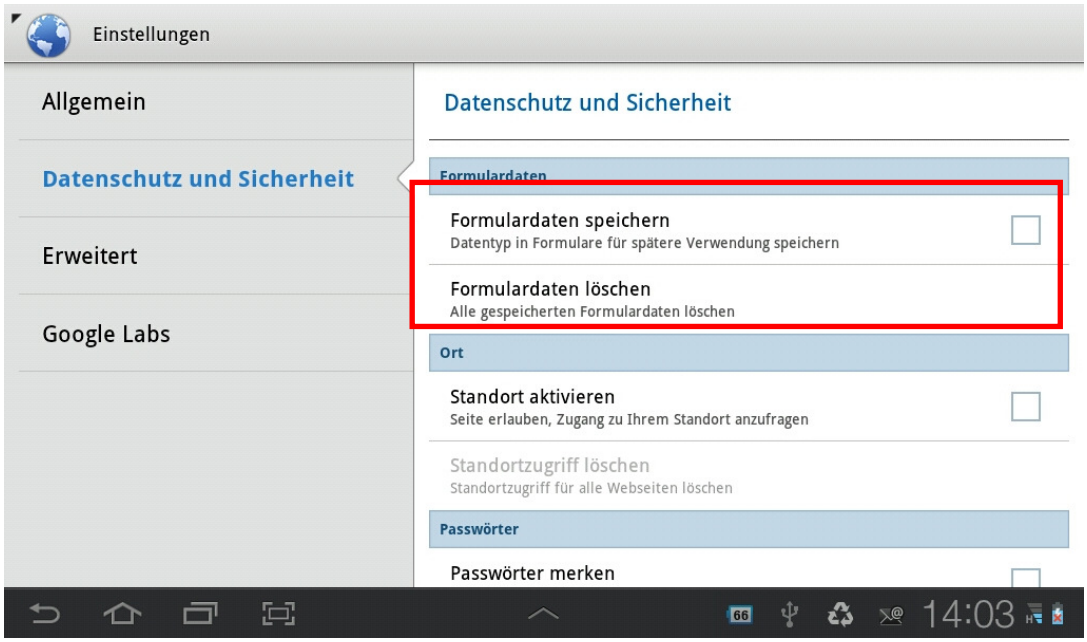




b) Formulardaten

Um zu vermeiden, dass andere Benutzer des Geräts auf die Daten zugreifen können, die Sie in die Formularfelder von Webseiten eingegeben haben, sollte die Funktion, diese Daten zu speichern, deaktiviert werden.

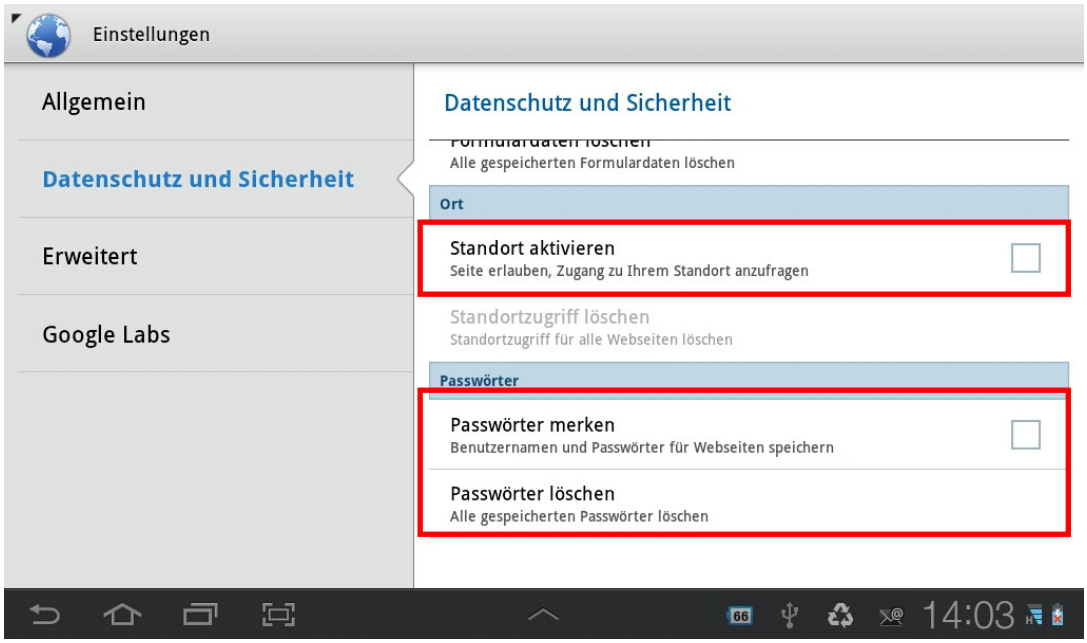
In der Browseranwendung: Einstellungen – Datenschutz und Sicherheit



c) Benutzernamen/Passwörter

Um zu vermeiden, dass Anmeldedaten für Webseiten oder Dienste von anderen Benutzern des Geräts genutzt werden, sollte die Funktion, diese Daten bei der Eingabe in Formularfelder zu speichern, deaktiviert werden.

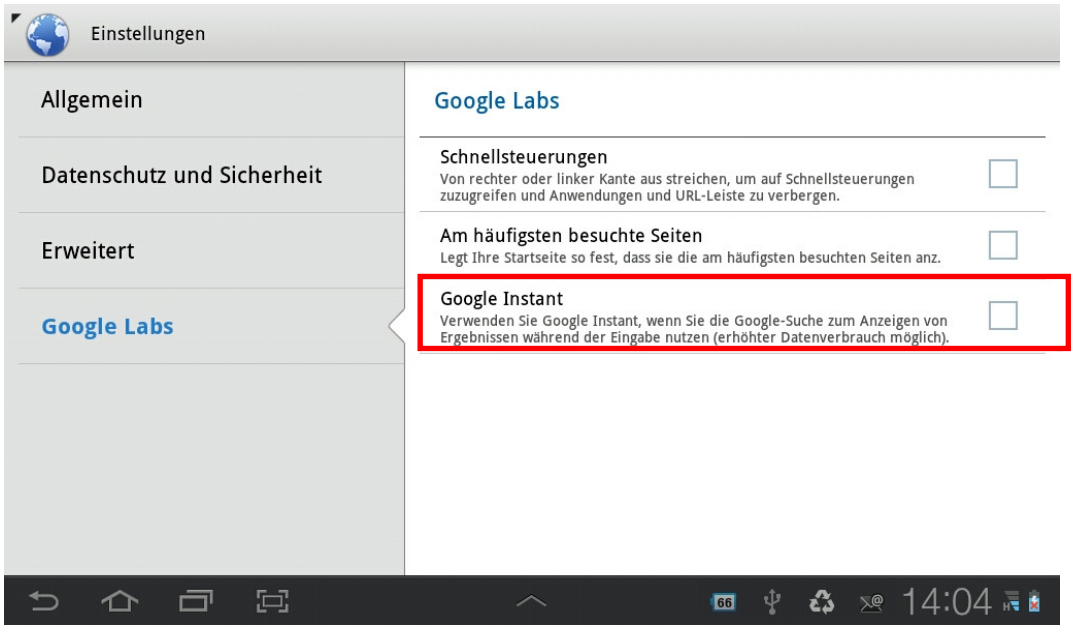
In der Browseranwendung: Einstellungen – Datenschutz und Sicherheit



d) Google Instant

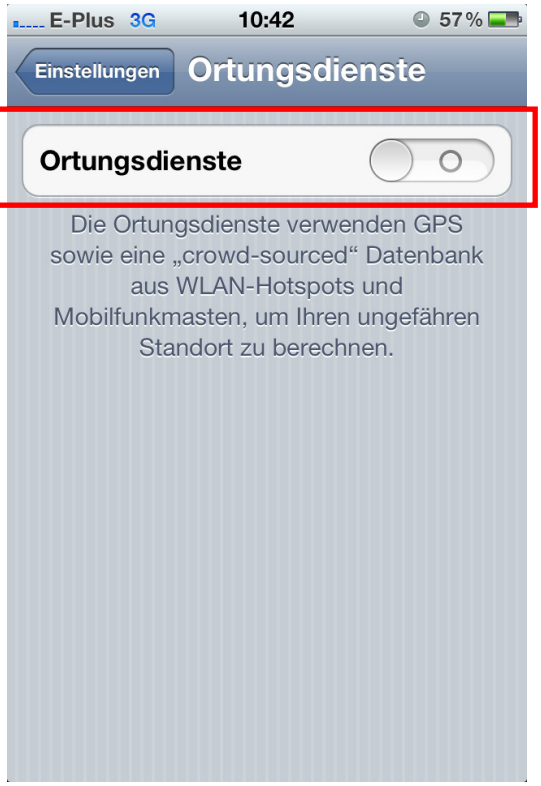
Um zu vermeiden, dass Google über den Browser erfährt, welche Webseiten Sie aufsuchen, sollte die Funktion „Google Instant“ deaktiviert werden

In der Browseranwendung: Einstellungen – Google Labs



B. Betriebssystem iOS (Version 5.1.1)

1. Ortungsdienste aktivieren/deaktivieren



Die GPS-Funktionalität (Ortungsdienste) sollte erst dann aktiviert werden, wenn Sie benötigt wird, um eine ungewollte Preisgabe des Standorts zu vermeiden.

Einstellungen – Ortungsdienste

2. Ortungsdienste für einzelne Programme zulassen/verbieten

iOS bietet die Möglichkeit, den Zugriff auf Standortdaten (GPS) gezielt nur bestimmten Anwendungen (Apps) zu erlauben.

Einstellungen – Ortungsdienste

3. Funknetz (WLAN) aktivieren/deaktivieren, Persönliche Hotspot-Funktion aktivieren/deaktivieren

Die WLAN-Funktionalität sollte erst dann aktiviert werden, wenn Sie benötigt wird, um eine ungewollte Preisgabe des Aufenthaltsorts zu vermeiden und Angriffsflächen zu reduzieren.

Einstellungen – WLAN-Netzwerke

Die Funktion, die Internet-Verbindung des Smartphones anderen Geräten zur Verfügung zu stellen, sollte erst aktiviert werden, wenn sie benötigt wird.

Einstellungen – Allgemein – Netzwerk– Persönlicher Hotspot

4. Nahfunk (Bluetooth) aktivieren/deaktivieren

Bei aktiverter Bluetooth-Funktion ist das Smartphone für andere Geräte in Ihrem Umfeld sichtbar und es können ggf. ungewollte Zugriffe erfolgen. Die Funktion sollte daher nur bei Bedarf aktiviert werden.

Einstellungen – Allgemein - Bluetooth

5. Smartphone mit Code-Sperre absichern

Um das Gerät vor einer unbefugten Nutzung zu schützen sollte das Smartphone mit einer Code-Sperre geschützt werden.

Einstellungen – Allgemein

Standardmäßig wird eine PIN aus vier Ziffern als Code-Sperre verwendet. Für eine höhere Sicherheit sollte die einfache Code-Sperre deaktiviert und ein Passwort aus Buchstaben und Ziffern verwendet werden.

Einstellungen – Allgemein - Code-Sperre

6. iCloud-Backup ausschalten bzw. konfigurieren

Bei der Nutzung der Cloud-Backup-Funktion von Apple werden die Inhalte des Smartphones auf den Servern von Apple in der iCloud gespeichert. Wenn man dies nicht möchte, sollte die Funktion deaktivert werden.

Einstellungen – iCloud – Speicher&Backup

Wenn die Funktion iCloud aktiviert sein sollte, lässt sich steuern, welche Daten auf diesem Weg gespeichert bzw. nicht gespeichert werden sollen.

Einstellungen – iCloud

7. SIM-Karten PIN aktivieren

Um die unbefugte Nutzung der Mobilfunkdienste des Smartphones zu nutzen, sollte die SIM-Karte mit einer PIN geschützt werden.

Einstellungen – Telefon – SIM-PIN

8. Datenschutzeinstellungen für den Browser „Safari“

a) Browser-Cache und -Verlaufsanzeige, Cookies

Um die Datenspuren des Smartphone-Browsers zu reduzieren bzw. zu löschen, sollten in regelmäßigen Abständen Browser-Speicher (Cache) und Browser-Verlauf gelöscht werden.

Einstellungen – Safari

Für Cookies lässt sich einstellen, in welchem Umfang diese akzeptiert werden.

Einstellungen – Safari – Cookies erlauben

b) Privates Surfen

Diese Datenspuren werden vermieden, wenn die Funktion „Privates Surfen“ aktiviert wird.

Einstellungen – Safari

c) Betrugswarnung, Pop-up-Fenster

Um Angriffsflächen zu reduzieren sollten die vorhandenen Warnfunktionen aktiviert, und Pop-Up-Fenster unterdrückt werden.

Einstellungen – Telefon – SIM-PIN

9. Allgemeine Datenschutzeinstellungen bei iOS 6.x

Die iOS-Version 6.x bietet die Möglichkeit, verschiedene Datenschutzeinstellungen an zentraler Stelle vorzunehmen.

Einstellungen – Datenschutz

Die iOS-Version 6.x bietet die Möglichkeit, verschiedene Datenschutzeinstellungen an zentraler Stelle vorzunehmen.

Einstellungen – Datenschutz – Ortungsdienste

Hier steht die Möglichkeit zur Verfügung den Zugriff auf Standort-, Kobtakt- und Kalenderdaten, Erinnerungen, Fotos und Bluetooth, Twitter- und Facebook-Accounts je App separat einzustellen.

10. Deaktivieren der Tracking-Möglichkeit durch Werbeanbieter.

Deaktivieren der Tracking-Möglichkeit durch Werbeanbieter.

Einstellungen – Allgmein – Info – Werbung

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

www.mjv.rlp.de/smartphones