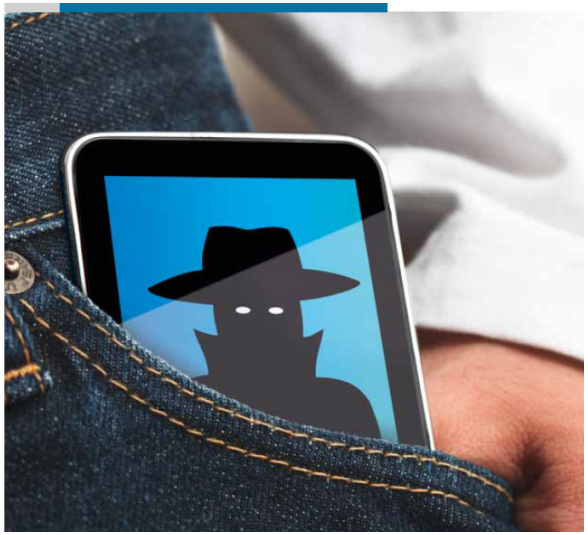
SMARTPHONES
UND APPS

Spione in der Hosentasche



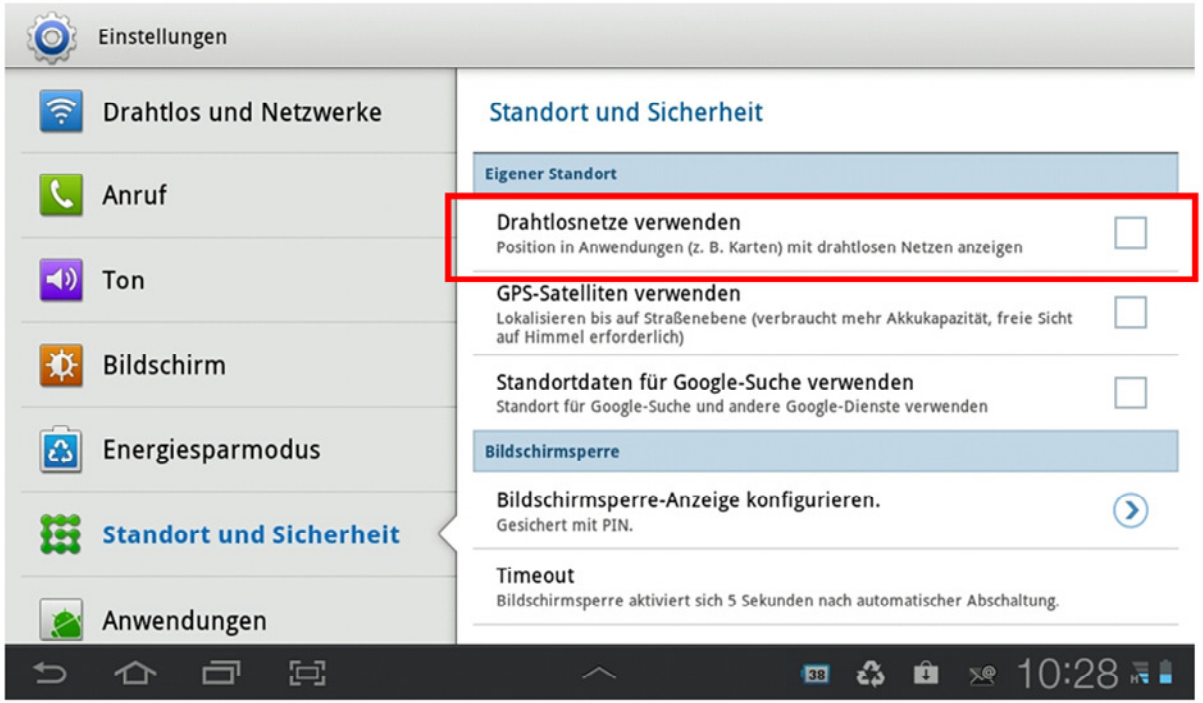
Datenschutzeinstellungen bei Smartphones (Android)

1. WLAN / Bluetooth
2. Standort
3. PIN – Passwort - Sperrmuster
4. SIM-Karten-Schutz
5. Geräteverschlüsselung
6. Browserdaten

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.

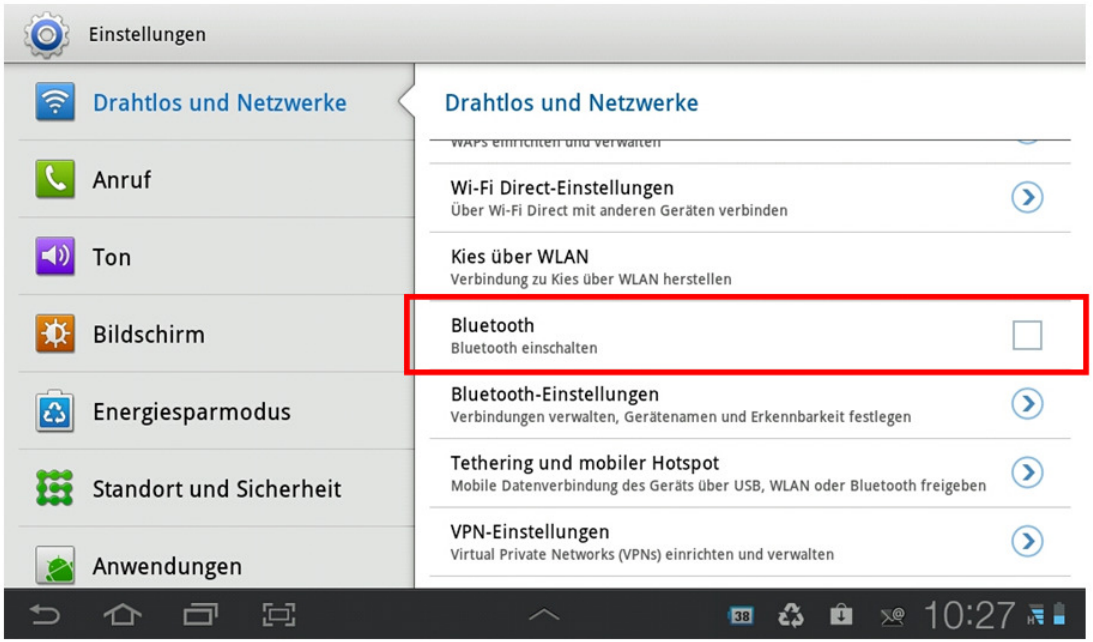
Einstellungen – Standort und Sicherheit



Bluetooth aktivieren / deaktivieren

Bei aktivierter 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.

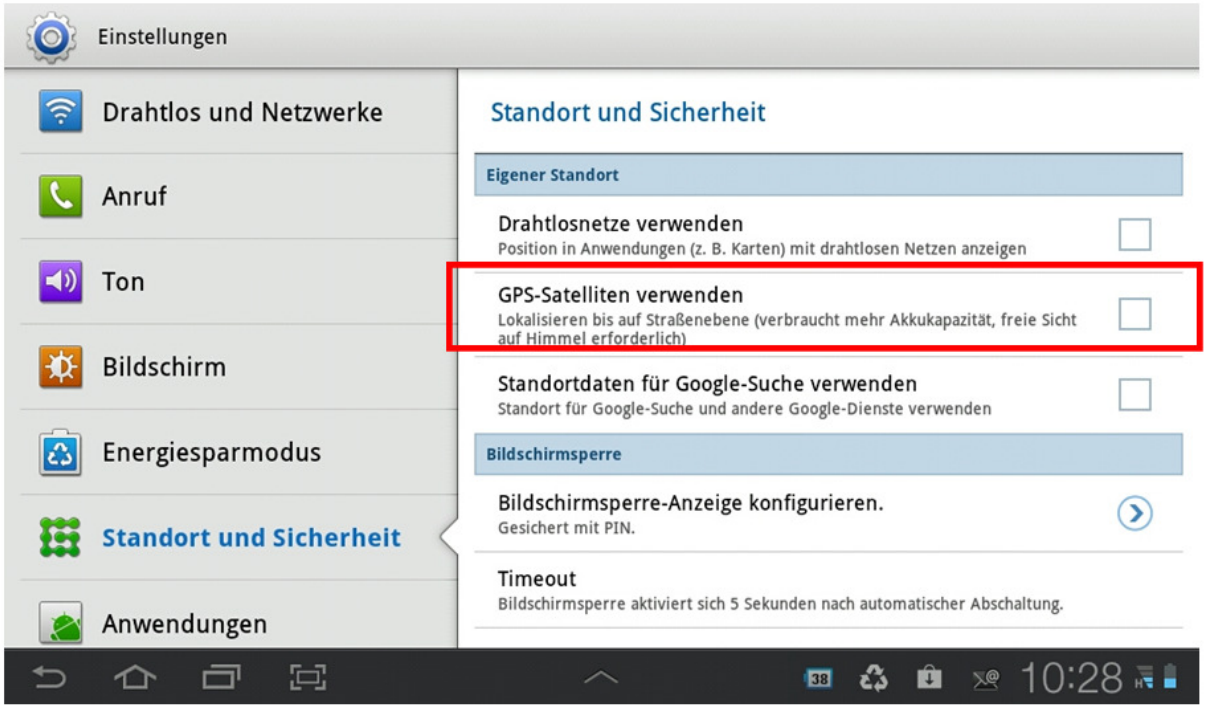
Einstellungen – Drahtlos und Netzwerke



Standortdaten (GPS) aktivieren / deaktivieren

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

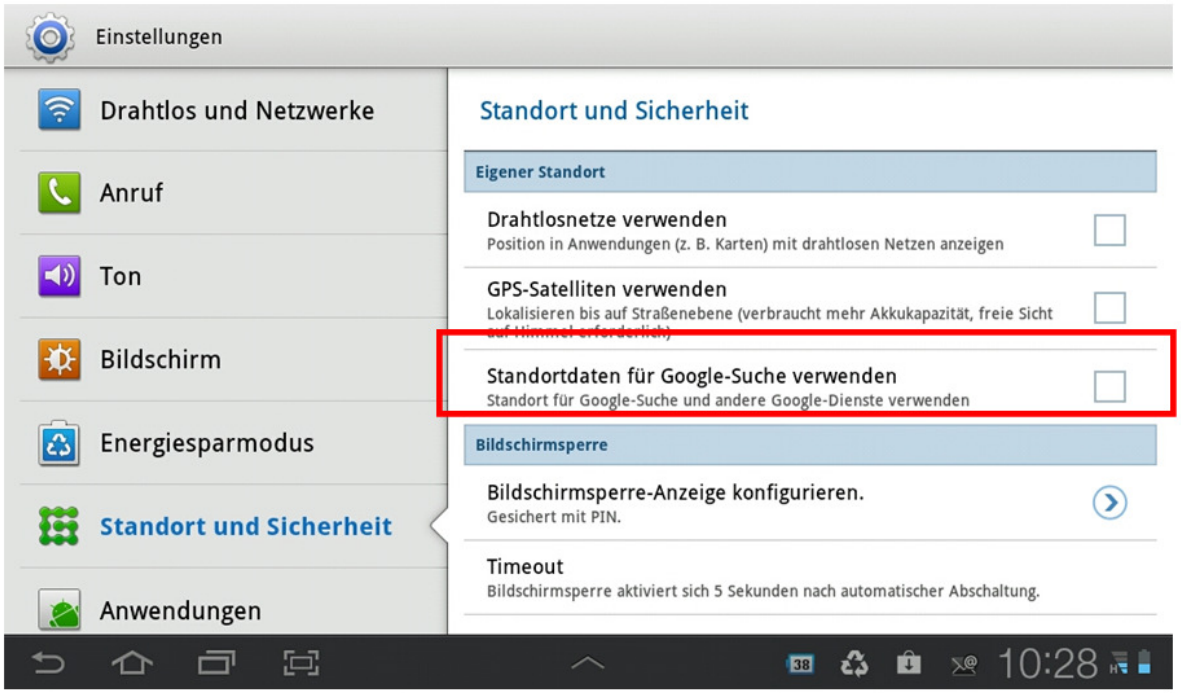
Einstellungen – Standort und Sicherheit



Standortdaten für die Google-Suche zulassen / verbieten

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

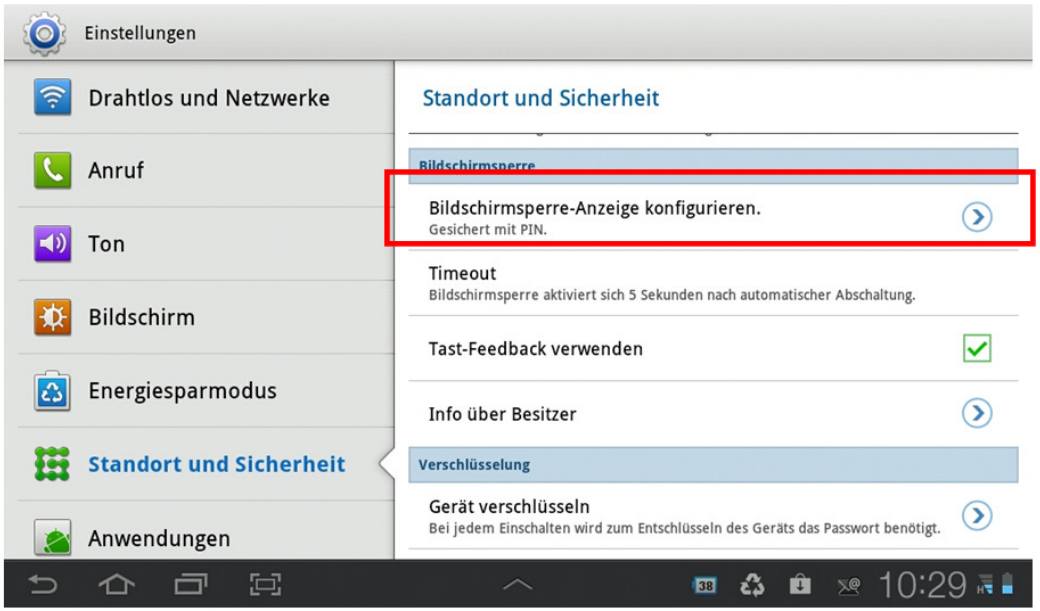
Einstellungen – Standort und Sicherheit



Geräte-PIN / Passwort / Sperrmuster einstellen - 1

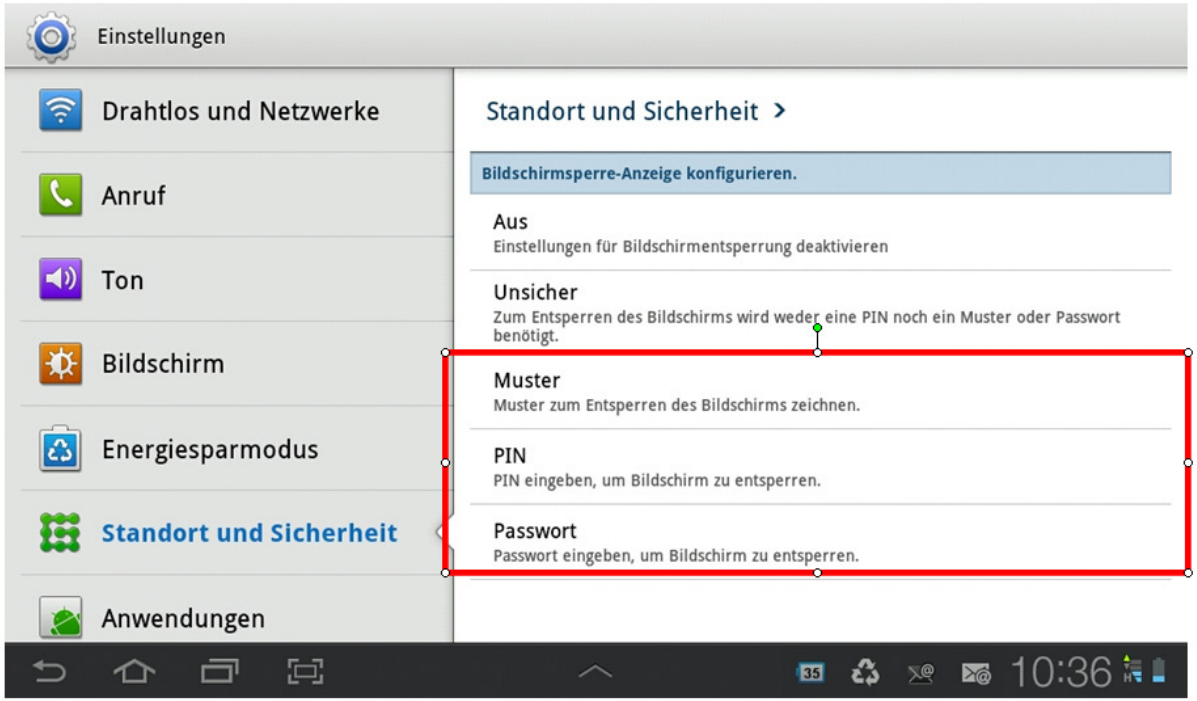
Um das Gerät vor einer unbefugten Nutzung zu schützen sollte das Smartphone mit einem Entsperrmuster, einer PIN oder einem Passwort geschützt werden.

Einstellungen – Standort und Sicherheit



Geräte-PIN / Passwort / Sperrmuster einstellen - 2

Einstellungen – Standort und Sicherheit – Bildschirmsperre-Anzeige konfigurieren

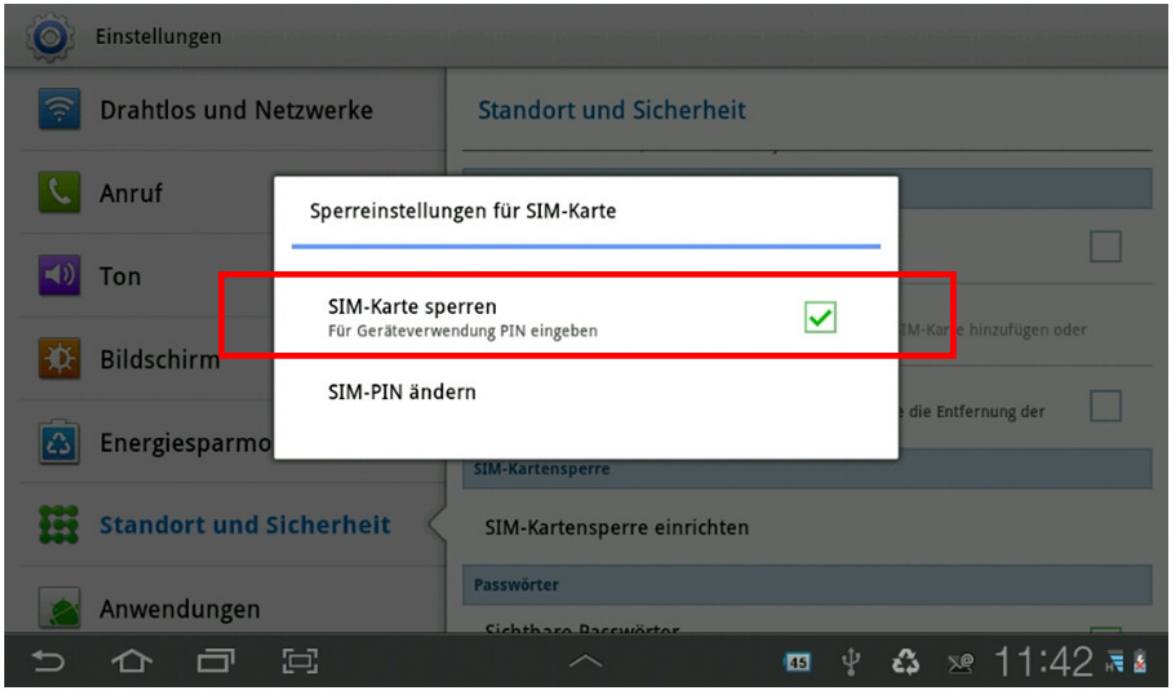


SIM-Karten-Schutz festlegen - 1

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

SIM-Karten-Schutz festlegen - 2



Geräteverschlüsselung aktivieren

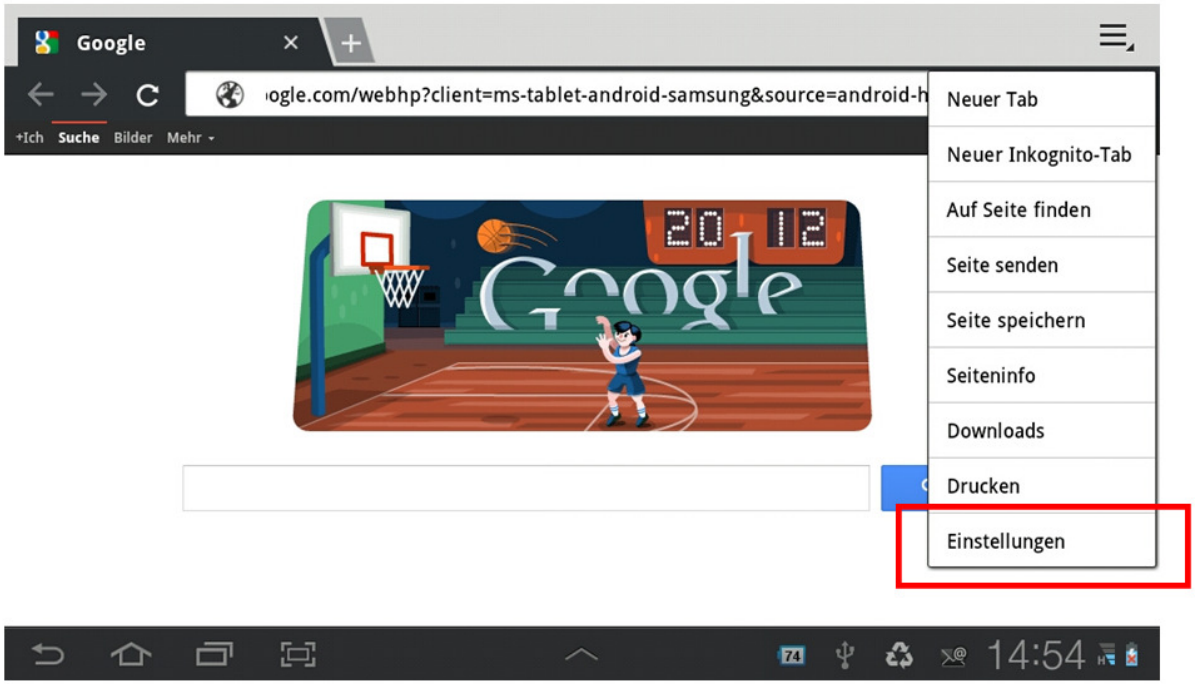
Um die Kenntnisnahme bei Verlust oder Diebstahl zu vermeiden, sollte die verschlüsselte Speicherung der Daten auf dem Smartphone aktiviert werden.

Einstellungen – Standort und Sicherheit

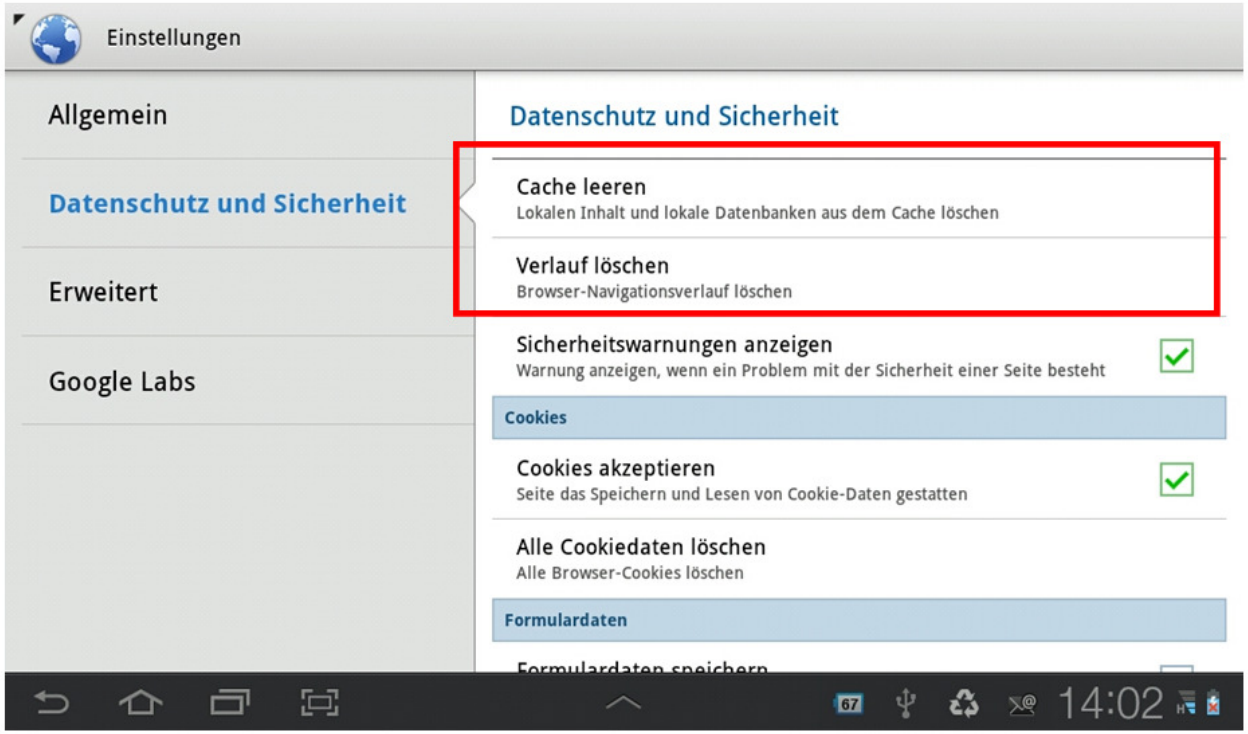
Browserspuren löschen - 1

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



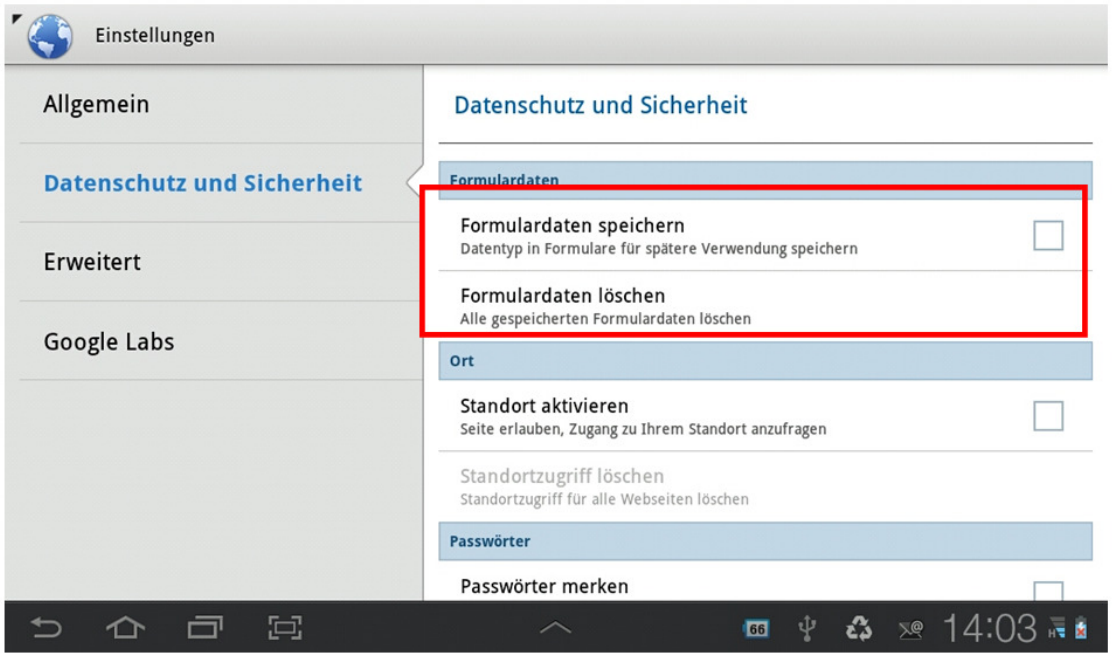
Browserspuren löschen - 2



Browserspuren löschen - 3

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.

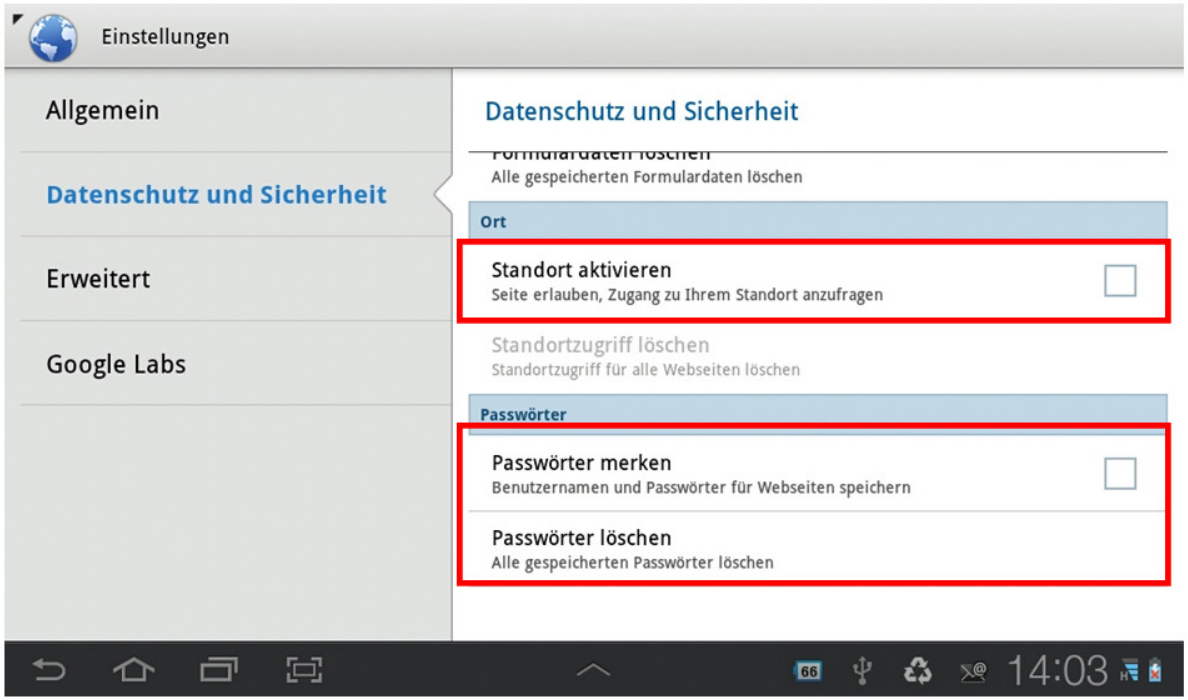
In der Browseranwendung: Einstellungen – Datenschutz und Sicherheit



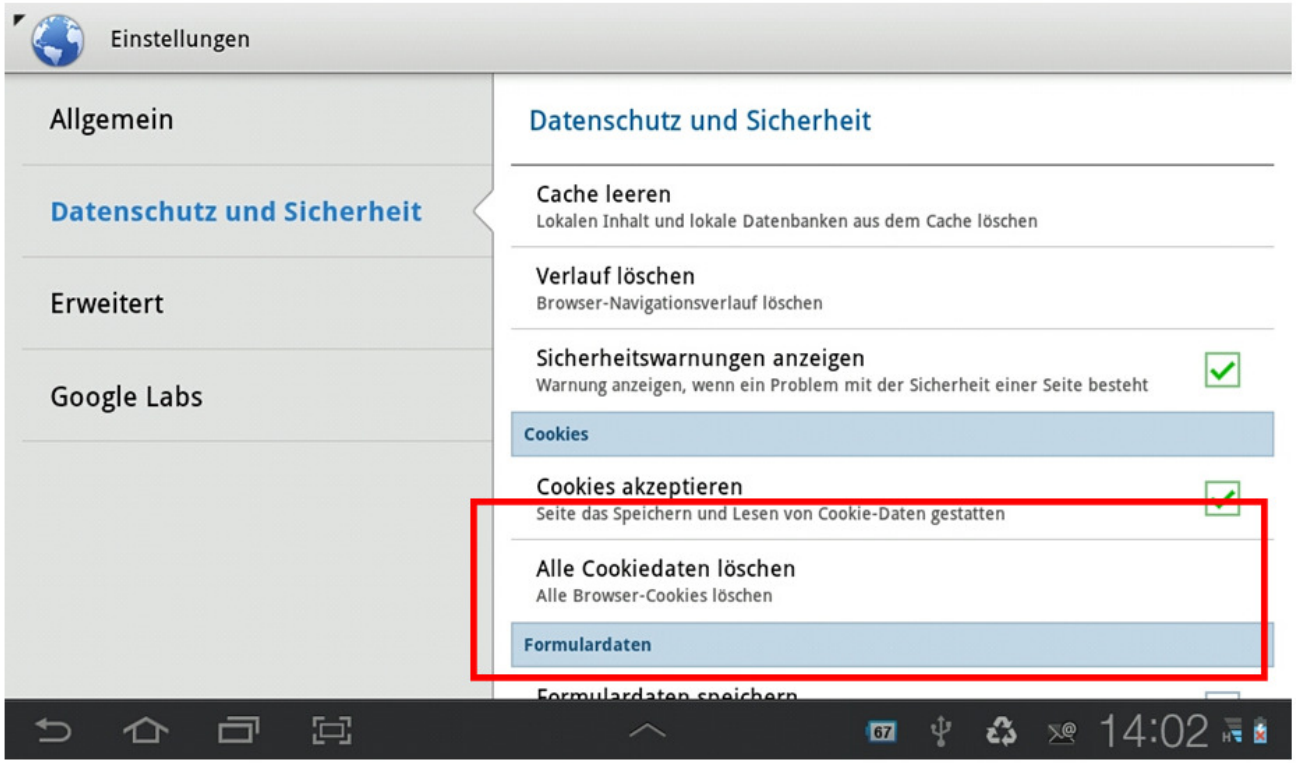
Browserspuren löschen - 4

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



Browserspuren löschen - 5



Internet-Angebot zu Smartphones
Datenschutzbeauftragter / Verbraucherschutz

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

www.mjv.rlp.de/smartphones