PRIVACY POLICY

TeaCapps “Barcode Scanner Apps”

1 - SCOPE, RESPONSIBLE ENTITY, LEGAL BASIS & RETENTION PERIOD

1.1 - SCOPE OF PRIVACY POLICY

This privacy policy explains the nature, purpose and scope of the collection and processing of personal data for the barcode scanner applications available under the following links:

https://play.google.com/store/apps/details?id=net.qrbot
https://play.google.com/store/apps/details?id=com.teacapps.barcodescanner
https://play.google.com/store/apps/details?id=com.teacapps.barcodescanner.pro
https://itunes.apple.com/app/id1048473097
https://itunes.apple.com/app/id909883348

1.2 - NAME AND ADDRESS OF RESPONSIBLE ENTITY

The responsible entity within the meaning of the General Data Protection Regulation and other national data protection laws is:
TeaCapps GmbH

Taläckerstraße 42
74182 Obersulm
GERMANY
CEO: Christian Wörz, Markus Wörz
info@teacapps.de

1.3 - SCOPE OF DATA PROCESSING

We collect and use personal information of our users to the extent necessary to provide high-quality applications and to perform our services, including the display of product and price information related to scanned barcodes.
In case where we make our services available free of charge, we finance our services through personalized advertising.

1.4 - LEGAL BASIS

When processing personal data that is required to fulfill a contract with the user, point (b) of paragraph 1 of article 6 of the GDPR serves as the legal basis.
If the processing is necessary to account for the legitimate interests of our company or a third party and if these interests are not overridden by interests of the user, the legal basis is provided by point (f) of paragraph 1 of article 6 of the GDPR.

1.5 - RETENTION PERIOD

The personal data of the user will be deleted as soon as the underlying purpose for the collection has been fulfilled. The information on the retention period is given individually for each data processing operation.

2 - DATA PROCESSING OPERATIONS

2.1 - FIREBASE HOSTING

Our apps use content from and link to websites hosted with Firebase Hosting, a service provided by Google LLC (“Google”). Hereby user data is send to the Firebase Hosting servers including IP addresses and user agent information. Firebase Hosting uses IP addresses of incoming requests to detect abuse and provide us with detailed analysis of usage data. The IP addresses are temporarily stored by Firebase hosting for several months. For more information see https://firebase.google.com/support/privacy/.

2.2 - GOOGLE ADSENSE

We use Google Adsense and show personalized ads within our barcode scanner apps to finance our development where apps are provided free of charge. Google Adsense stores user data including IP address and other personal data which can be used to identify the user's browser for the purpose of billing advertisers for ad clicks and detecting fraudulent clicks. The IP address will be anonymized after 9 months. For more information about Google Adsense and how to opt-out of personalized ads see https://policies.google.com/technologies/partner-sites.

2.3 - GOOGLE ANALYTICS FOR FIREBASE

We use Google Analytics for Firebase to learn more about how our users interact with our apps. This helps us to improve our apps in areas where they are most relevant to our users. Anonymous data about how users behave is automatically sent to Google Analytics for Firebase servers. Such data includes Mobile ad IDs, IDFVs/Android IDs, Instance IDs, Analytics App Instance IDs and the type (EAN, UPC, QR, ..) of scanned barcodes. For more information see Data collection. Sent data DOES NOT include the content of the scanned barcode or any other personal information such as name, email address or phone number. The ID-associated data will be stored for 60 days. Aggregated reporting and campaign data will be stored for up to 14 months. The collection of data can be deactivated in the settings of our barcode scanner apps by unchecking "Usage statistics".

2.4 - FIREBASE REMOTE CONFIG

We use individual app configurations for our users with the aid of Firebase Remote Config, for example to show country-specific website links. Firebase Remote Config uses Instance IDs to select configuration values to return to end-user devices. These Instance IDs will be stored up to 180 days.

2.5 - CRASHLYTICS

We use "Crashlytics" from Google. Crashlytics identifies software errors and their causes. Crashlytics collects the following data: device state information, device type, device ID and stores it anonymously for up to 3 years. The purpose of the data collection is the identification of software errors and their causes. For more information about the Crashlytics privacy notices see https://try.crashlytics.com/terms/privacy-policy.pdf

2.6 - LINKS TO WEBSITES

When scanning product barcodes with the EAN or UPC format our barcode scanner apps may show links to external websites which can be used to obtain product and price information related to the scanned barcodes. When following these links, the barcode number and the user's IP address and browser/device information will be transmitted to and may be stored by the respective websites. In the case where these websites offer an interface (API) to retrieve product and price information, this data is also transmitted when users do not follow these links. This allows users to see relevant product and pricing information without leaving our apps. This automatic retrieval of product and price information can be turned off in the app settings. In addition, we participate in affiliate programs offered by some websites we link to. In these cases, the links will contain a marker tag indicating that the user is from our app. The websites offering the affiliates will pay us a commission, if the users purchases products on the linked website. Users do not pay a higher price when using affiliate links.

2.7 - APPLE ICLOUD

Within our iOS apps users may optionally store scanned barcode data in their personal Apple iCloud folder. Apple's iCloud privacy policy applies in this context. We do not have access to our users' personal iCloud folder. Saving their data in iCloud let's users automatically synchronize their scan data across multiple devices.

2.8 - EMAIL CONTACT

Users may send us an email either directly or using forms within the apps. Personal data transmitted by email will be stored. In this context, data will not be disclosed with third parties. The data is used exclusively for processing the conversation. The data will be deleted, if the purpose of its collection has been fulfilled. This is the case when the conversion with the user has come to an end or it can be seen from the conversation that the subject has been clarified.