STRICH

PRIVACY AND SECURITY STATEMENT

Last updated: July 2026

Overview

This document describes its privacy and security-related aspects.

Runtime Architecture

STRICH is an SDK for reading 1D/2D codes in web apps running in a web browser, typically on a smartphone. The code of STRICH is included in your app, either via bundling, or by loading it dynamically, similar to a charting library.
The data STRICH receives are images from the smartphone's camera. It attempts to read barcodes from these images, and returns them to the host app.
All of this processing happens **on the device**, within the security boundary of your app. The data is **not sent** to our servers.

Camera Access

To perform barcode recognition, the SDK requires access to the device camera. Browsers and operating systems control access to the camera via a permission system, typically involving an end-user prompt to confirm access. In addition, browsers enforce a secure origin (HTTPS) for apps that access the camera.

For more in-depth technical information on this topic, please refer to the MDN Article on getUserMedia() privacy and security.

Data in Transit

The SDK transmits data to our license service for two reasons: *online license verification* and *usage tracking*. All data is protected in transit via industry-standard TLS connections (Qualys SSL Labs grade A).

Online License Verification

During initialization, the SDK performs a license check of the license key with our servers, and sends a number of non-identifying characteristics of the browser:

- License key
- Origin URL (to verify if the URL is included in the scope of the license)
- User-Agent (for statistical purposes)
- SDK version (for statistical purposes)
- Device ID (a randomly generated identifier)

Due to the nature of TCP/IP networking, we also receive the client IP address, but discard it immediately.

> 💡 STRICH Business and STRICH Enterprise licenses can purchase an optional *Offline Operation* add-on, which allows the license verification to happen fully offline, with no network requests involved.

Usage Tracking

To track the usage in our metered licenses (STRICH Basic and STRICH Professional), the SDK periodically transmits the number of scans and the types of barcodes that were scanned.

In addition the data sent during online license verification, the following information is sent to our servers for usage tracking:

- Timestamp: the instant in time when the scan occurred
- Symbology: the type of barcode scanned (Code 128, QR Code, etc.)
- Integration: an internal identifier telling us which module of the library was responsible for acquiring the barcode, e.g. PopupScanner

The values encoded in the barcodes are not sent.

💡STRICH Business and STRICH Enterprise licenses allow opting out of usage tracking, as these licenses include an unlimited number of scans, we have no need to track usage and consequently do not do so.

You can elect to voluntarily send usage data to be able to view scanning statistics in the Customer Portal and export them to CSV, but it is optional.

Data at Rest

The SDK stores the following data locally:

- A randomly generated device identifier in localStorage, used for statistical purposes, to calculate an estimated amount of devices
- A token that represents a stored license check result

None of this data is in any way sensitive or identifiable.