



## 2WIN-S und 2WIN-S Plus entsprechen der GDPR

Bei Adaptica kümmern wir uns um Daten. Wir schützen Ihre Daten und die Daten Ihrer Kunden. Dieses Dokument erklärt die Datenschutz- und Sicherheitsfunktionen von 2WIN und 2WIN-S Plus und gibt Hinweise, wie man die Sicherheit der Daten weiter verbessern kann.

### 2WIN-S und 2WIN-S Plus Sicherheitsmerkmale

2WIN-S und 2WIN-S Plus bestehen beide aus einer 2WIN-Vision-Screening-Kamera, einem Kaleidos-Röhrchen und einem Kontrolltablett mit der KALEIDOS App BT. Dies sind die Merkmale und Spezifikationen hinsichtlich der Sicherheit der in den beiden Geräten gespeicherten Daten.

- Das 2WIN-S führt nur anonyme Untersuchungen durch, es werden also keine persönlichen Daten im Gerät gespeichert.
- In der KALEIDOS App BT ist es möglich, Patientendaten einzugeben (verfügbar ab Softwareversion 5.4). Diese Daten werden nicht an das 2WIN-S gesendet und bleiben im Kontrolltablett gespeichert.
- Die KALEIDOS App BT funktioniert nur, wenn eine Sicherheitssperre im Steuertablett eingerichtet ist. Die App warnt den Benutzer, wenn die Sicherheitssperre nicht eingerichtet ist, und startet erst, wenn diese eingerichtet ist.
- Die KI-Anwendung (verfügbar ab Softwareversion 5.5.0) sendet und speichert nur anonyme Daten und gegebenenfalls die für den Service erforderliche Mindestmenge.
- Für die EMR-Integration (verfügbar ab Softwareversion 5.5.0) muss der Benutzer einen gemeinsamen Ordner einrichten. Dies muss mit dem Samba-Protokoll erfolgen und erfordert, dass ein Passwort für den gemeinsamen Ordner festgelegt wird.
- In dem gemeinsamen Ordner wird jeweils nur eine Untersuchung gespeichert, um zu vermeiden, dass mehrere Untersuchungen durchgeführt werden, die nicht unter der direkten Kontrolle der Anwendung stehen.

### Hinweise zur Verbesserung der Sicherheit

Um die Sicherheit der Daten zu verbessern, werden die folgenden Maßnahmen dringend empfohlen.

1. Verschlüsseln Sie Ihr Bedientablett mit einer sicheren ID oder einem Passwort.  
2WIN-S Plus wird mit einer speziellen Fernbedienungskonsole (Tablet) geliefert, die bereits mit einem Standardpasswort verschlüsselt ist. Wir möchten jedoch, dass Sie Ihr eigenes Passwort einrichten, damit nur Sie auf Ihre Daten zugreifen können. Im Falle eines Diebstahls des Geräts würde dies verhindern, dass Fremde auf die Daten zugreifen können.  
Wählen Sie eine geeignete Sicherheitssperre, z. B. eine ID mit mindestens 6 Ziffern oder ein Passwort mit mindestens 8 Zeichen, einschließlich Großbuchstaben, Zahlen und Symbolen.
2. Der gleiche Ratschlag für das Passwort gilt auch für den Schutz des gemeinsamen EMR-Ordners.
3. Um den EMR-Freigabeordner zu schützen, aktualisieren Sie regelmäßig den PC oder Server, von dem aus der Freigabeordner eingerichtet wird, mit den neuesten Betriebssystem-Sicherheitspatches.